

(51) 国際特許分類7
G06F 15/02

A1

(11) 国際公開番号

WO00/49510

(43) 国際公開日

2000年8月24日(24.08.00)

(21) 国際出願番号

PCT/JP00/00904

(22) 国際出願日

2000年2月17日(17.02.00)

(30) 優先権データ

特願平11/39218

1999年2月17日(17.02.99)

JP

(71) 出願人 (米国を除くすべての指定国について)

ソニー株式会社(SONY CORPORATION)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)

(72) 発明者; および

(75) 発明者/出願人 (米国についてののみ)

河上 達(KAWAKAMI, Itaru)[JP/JP]

石黒隆二(ISHIGURO, Ryuji)[JP/JP]

田辺 充(TANABE, Mitsuru)[JP/JP]

江面裕一(EZURA, Yuichi)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号

ソニー株式会社内 Tokyo, (JP)

(74) 代理人

小池 晃, 外(KOIKE, Akira et al.)

〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル

Tokyo, (JP)

(81) 指定国 AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

添付公開書類

国際調査報告書

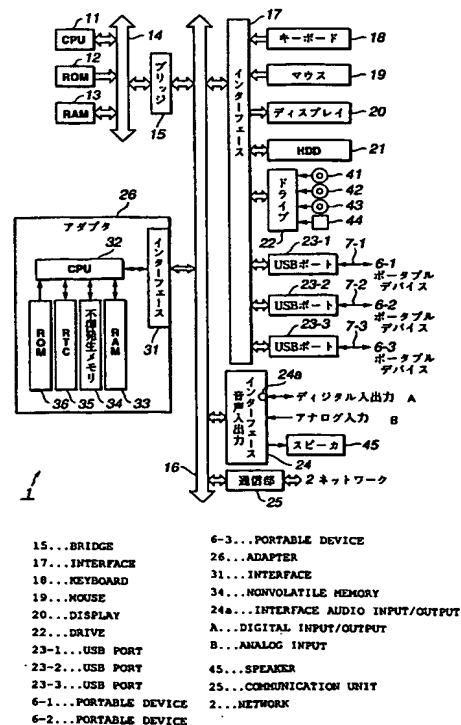
補正書

(54)Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROGRAM STORAGE MEDIUM

(54)発明の名称 情報処理装置及び方法並びにプログラム格納媒体

(57) Abstract

A CPU (11) of a personal computer (1) instructs a CPU (32) of an adapter (26) comprising a semiconductor IC to calculate the hash value of a tune database for managing the contents recorded on an HDD (21) and to store the hash value in a nonvolatile memory (34). When the contents recorded on the HDD (21) are reproduced, the CPU (11) calculates the hash value of the tune database, compares it with the hash value stored in the nonvolatile memory (34), and control the reproduction of the contents from the HDD (21) according to the results of the comparison.



パーソナルコンピュータ 1 の CPU 1 1 は、HDD 2 1 に記録されているコンテンツを管理する曲データベースのハッシュ値を、半導体 IC よりなるアダプタ 2 6 の CPU 3 2 により演算させ、不揮発性メモリ 3 4 に記憶させる。HDD 2 1 に記録されているコンテンツを再生するとき、CPU 1 1 は、HDD 2 1 の曲データベースのハッシュ値を計算し、不揮発性メモリ 3 4 に記憶されているそれまでのハッシュ値と比較し、その比較結果に対応して、HDD 2 1 からのコンテンツの再生を制御する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボワール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェッコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

明細書

情報処理装置及び方法並びにプログラム格納媒体

技術分野

本発明は、情報処理装置及び方法並びにプログラム格納媒体に関し、特に、改竄を防止し、不正な複製を抑制することができるようにした、情報処理装置及び方法並びにプログラム格納媒体に関する。

背景技術

最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種のデータがデジタル的に記録媒体に記録又は再生されるようになってきた。その結果、複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが可能となってきた。

しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

(1) 例えば、コンパクトディスク(CD)からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができて

しまう。

－(2) CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピーの回数に制限がないため、複製が大量に配布されてしまう。

(3) パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、ポータブルデバイスなどの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

(4) 上記した(3)の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように(いわゆる、音楽データをムーブするように)パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば、ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

(5) パーソナルコンピュータが、ハードディスク内のデジタル音楽データをポータブルデバイスなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

(6) ポータブルデバイスなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御しているソフトウェアがどのようなソフトウェアであるかを確認しないため、違法なソフトウェアに対してデジタル音楽データが渡されてしまう恐れがある。

(7) CDより再生された音楽データをパーソナルコンピュータで取り扱うとき、複数の曲が同一か否かを判断するために、曲データに含まれるISRC(International Standard Recording Code)を使用することが可能であるが、CDによっては、ISRCデータを含んでいないものがある。この場合、複数の曲が同一であるか否かを判定することができなくなる。

(8) 以上のような各機能は、パーソナルコンピュータ上で、ソフトウェアの制御により実現されるため、そのソフトウェアが改竄されると、システムの作成者が意図しない動作を行わせることができてしまう。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、ソフトウェアを解析し、改竄することで、不正な複製が大量に生成されてしまうようなことを確実に防止することができるようにするものである。

本発明に係る情報処理装置は、コンテンツデータを蓄積する蓄積手段と、蓄積手段に対するコンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を制御手段に供給する、制御手段とは独立したハードウェアに設けられた実行手段とを含み、制御手段は、実行手段の実行結果に基づいて、蓄積手段に対するコンテンツデータの蓄積又は読み出しを制御

することを特徴とする。この情報処理装置において、蓄積手段は、蓄積しているコンテンツデータを管理する管理情報も蓄積しており、制御手段は、実行手段に、管理情報に基づいて所定の演算を実行させるようにすることができる。また、制御手段は、CPUとし、蓄積手段は、ハードディスクとし、実行手段は、制御手段としてのCPUとは別の半導体ICに組み込まれたCPUとすることができる。

本発明に係る情報処理方法は、制御手段は、実行手段の実行結果に基づいて、蓄積手段に対するコンテンツデータの蓄積又は読み出しを制御する制御ステップを含むことを特徴とする。

本発明に係るプログラム格納媒体のプログラムは、実行手段の実行結果に基づいて、蓄積手段に対するコンテンツデータの蓄積又は読み出しを制御する制御ステップを含むことを特徴とする。

また、本発明に係る情報処理装置は、コンテンツデータを入力する入力手段と、前記入力手段により入力されたデータを蓄積する蓄積手段と、前記蓄積手段に蓄積するデータを所定の方式で圧縮する圧縮手段と、前記蓄積手段に蓄積するデータを所定の方式で暗号化する暗号化手段と、前記圧縮手段により圧縮され、かつ前記暗号化手段により暗号化された前記データの、前記蓄積手段に対する蓄積又は読み出しを制御する制御手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、データを入力する入力ステップと、前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理

により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含むことを特徴とする。

また、本発明に係るプログラム格納媒体は、データを入力する入力ステップと、前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とする。

また、本発明に係る情報処理は、コンテンツデータを入力する入力手段と、前記入力手段により入力されたデータを蓄積する蓄積手段と、前記蓄積手段に蓄積されたデータの管理情報を保持する保持手段と、前記保持手段に保持されている前記管理情報に基づき所定の演算を行う演算手段と、前記演算手段の演算結果を記憶する記憶手段と、前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結果と比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの利用を制御する制御手段を含むことを特徴とする。

また、本発明に係る除法処理方法は、データを入力する入力ステップと、前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果と比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含むことを特徴とする。

また、本発明に係るプログラム格納媒体は、データを入力する入力ステップと、前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、前記演算ステップでの演算結果を記憶する記憶ステップと、前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果と比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とする。

また、本発明に係る情報処理装置は、他の装置との間でデータを授受する授受手段と、所定の固定鍵と保存用鍵を保持する保持手段と、前記他の装置との間でデータを授受するとき、前記保持手段に保持されている前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証手段と、前記通信用鍵を前記保存用鍵で暗号化する暗号化手段と、前記授受手段により受信された、前記通信用鍵で暗号化されているデータを、前記暗号化手段により暗号化された前記通信用鍵と対応させて蓄積する蓄積手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、他の装置との間でデータを授受する授受ステップと、所定の固定鍵と保存用鍵を保持する保持ステップと、前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とする。

また、本発明に係るプログラム格納媒体は、他の装置との間でデータを授受する授受ステップと、所定の固定鍵と保存用鍵を保持する保持ステップと、前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とする。

また、本発明に係る情報処理装置は、データを蓄積する蓄積手段と、前記蓄積手段に蓄積されている前記データの利用時の条件を保持する保持手段と、前記蓄積手段に蓄積されている前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定手段と、前記判定手段の判定結

果に基づいて、前記蓄積手段に蓄積されている前記データを前記保持手段に保持されている前記データの利用時の条件とともに前記他の装置に移転する移転手段とを含むことを特徴とする。

また、本発明に係る情報処理方法は、データを蓄積する蓄積ステップと、前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含むことを特徴とする。

さらに、本発明に係るプログラム格納媒体は、データを蓄積する蓄積ステップと、前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とする。

図面の簡単な説明

図 1 は、本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。

図 2 は、上記コンテンツデータ管理システムにおけるパーソナルコンピュータの構成を説明する図である。

図 3 は、コンテンツデータ管理システムにおけるポータブルデバイスの構成を説明する図である。

図 4 は、上記パーソナルコンピュータの機能の構成を説明するブロック図である。

図 5 は、表示操作指示ウィンドウの例を示す図である。

図 6 は、録音プログラムがディスプレイに表示させるウィンドウの例を説明する図である。

図 7 は、コンパクトディスクから H D D にコンテンツをコピーする場合の処理を説明するフローチャートである。

図 8 は、図 7 のフローチャートにおけるステップ S 1 2 の期限データベースチェック処理を説明するフローチャートである。

図 9 は、期限データベースの例を示す図である。

図 1 0 は、ウォータマークを説明する図である。

図 1 1 は、曲データベースの例を示す図である。

図 1 2 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図 1 3 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図 1 4 は、H D D からポータブルデバイスへコンテンツを移動する動作を説明するフローチャートである。

図15は、図12のフローチャートにおけるステップS55の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

図16は、ポータブルデバイス管理している再生条件を説明する図である。

図17は、図12のフローチャートにおけるステップS58のフォーマット変換処理の詳細を説明するフローチャートである。

図18は、HDDからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図19は、HDDからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図20は、HDDからポータブルデバイスへコンテンツをコピーする場合の動作を説明するフローチャートである。

図21は、ポータブルデバイスからHDDへコンテンツを移動する場合の動作を説明するフローチャートである。

図22は、ポータブルデバイスからHDDへコンテンツをコピーする場合の動作を説明するフローチャートである。

図23は、EMDサーバからHDDへコンテンツをコピーする場合の処理を説明するフローチャートである。

図24は、図23のフローチャートにおけるステップS204の課金に関する処理の詳細を説明するフローチャートである。

図25は、課金ログを説明する図である。

図26は、パーソナルコンピュータのIEC60958端子からHDDへコンテンツをコピーする場合の処理を説明するフローチャートである。

図 2 7 は、パーソナルコンピュータの I E C 6 0 9 5 8 端子から H D D へコンテンツをコピーする場合の処理を説明するフローチャートである。

図 2 8 は、H D D から I E C 6 0 9 5 8 端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図 2 9 は、H D D から I E C 6 0 9 5 8 端子にコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 0 は、図 2 8 のフローチャートにおけるステップ S 2 7 5 の再生条件などのチェック処理を説明するフローチャートである。

図 3 1 は、H D D からポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 2 は、H D D からポータブルデバイス経由でコンテンツを出力する場合の動作を説明するフローチャートである。

図 3 3 は、不揮発性メモリの機能を説明する図である。

図 3 4 は、アダプタの動作を説明するフローチャートである。

図 3 5 は、アダプタの内部の構成を示す図である。

図 3 6 A 及び図 3 6 B は、不揮発性メモリの内部の構成例を示す図である。

図 3 7 は、不揮発性メモリの内部の構成例を示す図である。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

図1は、本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワーク又はインターネットなどから構成されるネットワーク2に接続されている。パーソナルコンピュータ1は、EMD(Electrical Music Distribution)サーバ4-1乃至4-3から受信した、又は後述するCD(Compact Disc)から読み取った楽音のデータ(以下、コンテンツと称する)を、所定の圧縮の方式(例えば、ATRAC3(商標))に変換するとともにDES(Data Encryption Standard)などの暗号化方式で暗号化して記録する。

パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス(Portable Device(PDとも称する))の台数(後述する、いわゆるチェックアウトできるPDの台数)を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ1は、そのコンテンツを再生できる。

又は、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス6-1乃至6-3にコピーしたとき、パーソナルコンピュータ1は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス6-1乃至6-3に記憶させることができる回数は、制限される場合がある。この場合、コピーできる回数は、増えることがない。

又は、利用条件のデータは、他のパーソナルコンピュータに移動

することができるなどを示す。ポータブルデバイス 6-1 乃至 6-3 にコンテンツを移動させた後、パーソナルコンピュータ 1 が記録しているコンテンツは使用できなくなる（コンテンツが削除されるか、又は利用条件が変更されて使用できなくなる）。

利用条件のデータの詳細は、後述する。

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、又は再生条件など）とともに、U S B (Universal Serial Bus) ケーブル 7-1 を介して、接続されているポータブルデバイス 6-1 に記憶させるとともに、ポータブルデバイス 6-1 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ 1 が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1 減らされる。チェックアウトできる回数が 0 のとき、対応するコンテンツは、チェックアウトすることができない。

パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、U S B ケーブル 7-2 を介して、接続されているポータブルデバイス 6-2 に記憶させるとともに、ポータブルデバイス 6-2 に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、暗号化して記録しているコンテンツを、コンテンツに関連するデータとともに、U S B ケーブル 7-3 を介して、接続されているポータブルデバイス 6-3 に記憶させるとともに、ポータブルデバイス 6-3 に記憶させたことに対応して、

記憶させたコンテンツに対応する利用条件のデータを更新する。

また、パーソナルコンピュータ 1 は、U S B ケーブル 7 - 1 を介して、接続されているポータブルデバイス 6 - 1 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6 - 1 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ 1 が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1 増やされる。

パーソナルコンピュータ 1 は、U S B ケーブル 7 - 2 を介して、接続されているポータブルデバイス 6 - 2 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6 - 2 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ 1 は、U S B ケーブル 7 - 3 を介して、接続されているポータブルデバイス 6 - 3 にパーソナルコンピュータ 1 がチェックアウトしたコンテンツを、ポータブルデバイス 6 - 3 に消去させて（又は、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

パーソナルコンピュータ 1 は、図示せぬ他のパーソナルコンピュータがポータブルデバイス 6 - 1 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6 - 2 にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ 1 は、他のパーソナルコンピュータがポータブルデバイス 6 - 3 に

チェックアウトしたコンテンツをチェックインできない。

—E M D登録サーバ3は、パーソナルコンピュータ1がE M Dサーバ4-1乃至4-3からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とE M Dサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、E M Dサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

E M Dサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、又は再生制限など）とともに、パーソナルコンピュータ1にコンテンツを供給する。E M Dサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ1にコンテンツを供給する。E M Dサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータとともに、パーソナルコンピュータ1にコンテンツを供給する。

E M Dサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一又は異なる圧縮の方式で圧縮されている。E M Dサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一又は異なる暗号化の方式で暗号化されている。

WWW(World Wide Web)サーバ5-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったC D（例えば、C Dのアルバム名、又はC Dの販売会社な

ど) 及び CD から読み取ったコンテンツに対応するデータ (例えば、曲名、又は作曲者名など) をパーソナルコンピュータ 1 に供給する。WWWサーバ 5-2 は、パーソナルコンピュータ 1 の要求に対応して、ネットワーク 2 を介して、コンテンツを読み取った CD 及び CD から読み取ったコンテンツに対応するデータをパーソナルコンピュータ 1 に供給する。

ポータブルデバイス 6-1 は、パーソナルコンピュータ 1 から供給されたコンテンツ (すなわち、チェックアウトされたコンテンツ) を、コンテンツに関連するデータ (例えば、曲名、又は再生制限など) とともに記憶する。ポータブルデバイス 6-1 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス 6-1 は、対応するコンテンツの再生を停止する。

使用者は、コンテンツを記憶したポータブルデバイス 6-1 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-2 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-2 は、コンテンツに関連するデータ

に基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-2 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

ポータブルデバイス 6-3 は、パーソナルコンピュータ 1 から供給されたコンテンツを、コンテンツに関連するデータとともに記憶する。ポータブルデバイス 6-3 は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス 6-3 をパーソナルコンピュータ 1 から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

以下、ポータブルデバイス 6-1 乃至 6-3 を個々に区別する必要がないとき、単にポータブルデバイス 6 と称する。

図 2 は、パーソナルコンピュータ 1 の構成を説明する図である。CPU (Central Processing Unit) 11 は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System) を実際に実行する。ROM (Read-only Memory) 12 は、一般的には、CPU 11 が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 13 は、CPU 11 の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらは CPU バスなどから構成されるホストバス 14 により相互に接続されている。

ホストバス 14 は、ブリッジ 15 を介して、P C I (Peripheral Component Interconnect/Interface) バスなどの外部バス 16 に接続されている。

キーボード 18 は、C P U 11 に各種の指令を入力するとき、使用者により操作される。マウス 19 は、ディスプレイ 20 の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ 20 は、液晶表示装置又は C R T (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。H D D (Hard Disk Drive) 21 は、ハードディスクを駆動し、それらに C P U 11 によって実行するプログラムや情報を記録又は再生させる。

ドライブ 22 は、装着されている磁気ディスク 41、光ディスク 42 (C D を含む)、光磁気ディスク 43、又は半導体メモリ 44 に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース 17、外部バス 16、ブリッジ 15 及びホストバス 14 を介して接続されている R A M 13 に供給する。

U S B ポート 23-1 には、U S B ケーブル 7-1 を介して、ポータブルデバイス 6-1 が接続される。U S B ポート 23-1 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、H D D 21、C P U 11、又は R A M 13 から供給されたデータ (例えば、コンテンツ又はポータブルデバイス 6-1 のコマンドなどを含む) をポータブルデバイス 6-1 に出力する。

U S B ポート 23-2 には、U S B ケーブル 7-2 を介して、ポータブルデバイス 6-2 が接続される。U S B ポート 23-2 は、

インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-2 のコマンドなどを含む）をポータブルデバイス 6-2 に出力する。

USB ポート 23-3 には、USB ケーブル 7-3 を介して、ポータブルデバイス 6-3 が接続される。USB ポート 23-3 は、インターフェース 17、外部バス 16、ブリッジ 15、又はホストバス 14 を介して、HDD 21、CPU 11、又は RAM 13 から供給されたデータ（例えば、コンテンツ又はポータブルデバイス 6-3 のコマンドなどを含む）をポータブルデバイス 6-3 に出力する。

IEC(International Electrotechnical Commission) 60958 端子 24a を有する音声入出力インタフェース 24 は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ 45 は、音声入出力インタフェース 24 から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

これらのキーボード 18 乃至音声入出力インタフェース 24 は、インターフェース 17 に接続されており、インターフェース 17 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介して CPU 11 に接続されている。

通信部 25 は、ネットワーク 2 が接続され、CPU 11、又は HDD 21 から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式の packets に格納して、ネッ

トワーク 2 を介して、送信するとともに、ネットワーク 2 を介して、受信したパケットに格納されているデータ（例えば、認証鍵、又はコンテンツなど）を CPU 11、RAM 13、又は HDD 21 に出力する。

半導体 IC として、一体的に形成され、パーソナルコンピュータ 1 に装着されるアダプタ 26 の CPU 32 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介してパーソナルコンピュータ 1 の CPU 11 と共働し、各種の処理を実行する。RAM 33 は、CPU 32 が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ 34 は、パーソナルコンピュータ 1 の電源がオフされた後も保持する必要があるデータを記憶する。ROM 36 には、パーソナルコンピュータ 1 から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35 は、計時動作を実行し、時刻情報を提供する。

通信部 25 及びアダプタ 26 は、外部バス 16、ブリッジ 15 及びホストバス 14 を介して CPU 11 に接続されている。

以下、USB ポート 23-1 乃至 23-3 を個々に区別する必要がないとき、単に、USB ポート 23 と称する。以下、USB ケーブル 7-1 乃至 7-3 を個々に区別する必要がないとき、単に USB ケーブル 7 と称する。

次に、ポータブルデバイス 6 の構成を図 3 を参照して説明する。電源回路 52 は、乾電池 51 から供給される電源電圧を所定の電圧の内部電力に変換して、CPU 53 乃至表示部 67 に供給することにより、ポータブルデバイス 6 全体を駆動させる。

USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1から転送されたコンテンツを含むデータを、内部バス58を介して、CPU53に供給する。

パーソナルコンピュータ1から転送されるデータは、1パケット当たり64バイトのデータから構成され、12Mbit/secの転送レートでパーソナルコンピュータ1から転送される。

ポータブルデバイス6に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されているとともに、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限及び再生回数カウンタなどが格納されている。コンテンツは、ATRAC3などの符号化方式で符号化され、暗号化されている。

ヘッダサイズは、ヘッダのデータ長（例えば、33バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、33,636,138バイトなど）を表す。

コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ1とポータブルデバイス6との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ1からポータブルデバイス6に送信される。

ポータブルデバイス6がUSBケーブル7を介してパーソナルコンピュータ1のUSBポート23に接続されたとき、ポータブルデバイス6とパーソナルコンピュータ1とは、相互認証の処理を実行

する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス 6 の D S P 5 9 は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ 1 が生成するある値（チャレンジ）に対して、ポータブルデバイス 6 がパーソナルコンピュータ 1 と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ 1 が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス 6 が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ 1 は不正を検出できる。

コンテンツ ID は、コンテンツに対応した、コンテンツを特定するための ID である。

コーデック ID は、コンテンツの符号化方式に対応した ID であり、例えば、コーデック ID ” 1 ” は、A T R A C 3 に対応し、コーデック ID ” 0 ” は、M P 3 (MPEG(Moving Picture Experts Group) Audio Layer-3) に対応する。

ファイル名は、コンテンツに対応するパーソナルコンピュータ 1 が記録しているコンテンツファイル（後述する）を A S C I I (American National Standard Code for Information Interchange) コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などを A S C

IIコードに変換したデータである。

再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時又は終了日時）又は回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、“1”が割り当てられ、再生が可能な期間が設定されているとき、“2”が割り当てられ、回数制限及び再生が可能な期間がいずれも設定されていないとき（いわゆる、買取りで購入されたとき）、“0”が割り当てられる。

開始日時及び終了日時は、再生制限データが“2”であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が“00040F”であり、終了日時が“00070F”であるとき、対応するコンテンツは、2000年4月15日から2000年7月15日まで、再生が可能である。

同様に、回数制限及び再生回数カウンタは、再生制限データが“1”又は“2”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が“02”であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが“01”であるとき、そのコンテンツが再生された回数は1回である。

例えば、再生制限データが“2”であり、開始日時が“00040F”であり、終了日時が“00070F”であり、回数制限が“02”であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間に

において、1日2回ずつ繰り返し再生できる。

例えば、再生制限データが”1”であり、開始日時が”000000”であり、終了日時が”000000”であり、回数制限が”0a”であり、再生回数カウンタが”05”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツとともにコンテンツの書き込み命令を受信した場合、ROM55からRAM54に読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

なお、フラッシュメモリ61は、ポータブルデバイス6にメモリカードとして着脱可能とすることができる。

使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードとコンテンツとを読み出させ、DSP59に転送させる。

DSP59は、フラッシュメモリ61から転送された再生用コードに基づいてコンテンツをCRC(Cyclic Redundancy Check)方式

で誤り検出をした後、再生して、再生したデータ（図3中においてD1で示す）をディジタル／アナログ変換回路63に供給する。

DSP59は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子59AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びに、フレーム単位のLチャンネルクロックLCLK及びRチャンネルクロックRCLKからなる動作クロックLRCLKをディジタルアナログ変換回路63に供給する。

DSP59は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路63に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

同様に、CPU53及びUSBコントローラ57も、水晶でなる発振子53A又は57Aがそれぞれ外付けされ、発振子53A又は57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

このように構成することで、ポータブルデバイス6は、CPU53、DSP59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

ディジタルアナログ変換回路63は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路64に供給する。増幅

回路 6 4 は、音声信号を増幅して、ヘッドフォンジャック 6 5 を介して、図示せぬヘッドフォンに音声信号を供給する。

このように、ポータブルデバイス 6 は、図示せぬ再生／停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいてフラッシュメモリ 6 1 に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

ポータブルデバイス 6 は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU 5 3 の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス 6 は、自動的に電源をオフして消費電力を低減する。

因みに、ポータブルデバイス 6 は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1 曲目から再生する。

また、ポータブルデバイス 6 の CPU 5 3 は、LCD コントローラ 6 8 を制御して、表示部 6 7 に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池 5 1 の残量等の情報を表示させる。

さらに、ポータブルデバイス 6 は、EEPROM 6 8 に、フラッシュメモリ 8 0 に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ 6 1 のブロック位置及びその他種々のメモリ蓄積情報等のいわゆる F A T (F i l e

A l l o c a t i o n T a b l e) を格納する。

—因みに、本実施の形態においては、コンテンツは、64 K B y t e を1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がF A Tに格納される。

フラッシュメモリ61にF A Tが格納される場合、例えば、1曲目のコンテンツがC P U 53の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がF A Tとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

このように、F A Tは、フラッシュメモリ61へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

F A Tがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書換えの回数に達してしまい、フラッシュメモリ61の書換えができなくなってしまう。

そこで、ポータブルデバイス6は、F A TをE E P R O M 68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書換えの頻度を少なくしている。

書換えの回数の多いF A TをE E P R O M 68に記憶させることにより、F A Tをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数

を数十倍以上に増やすことができる。更に、CPU 53は、EEPROM 68にFATを追記するように書き込ませるので、EEPROM 68の同一の領域の書換えの頻度を少なくして、EEPROM 68が短期間で書換え不能になることを防止する。

ポータブルデバイス 6は、USBケーブル 7を介してパーソナルコンピュータ 1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ 57からCPU 53に供給される割り込み信号に基づき、USB接続されたことを認識する。

ポータブルデバイス 6は、USB接続されたことを認識すると、パーソナルコンピュータ 1からUSBケーブル 7を介して規定電流値の外部電力の供給を受けるとともに、電源回路 52を制御して、乾電池 51からの電力の供給を停止させる。

CPU 53は、USB接続されたとき、DSP 59のコンテンツの再生の処理を停止させる。これにより、CPU 53は、パーソナルコンピュータ 1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

このようにCPU 53は、USB接続されると、乾電池 51から供給される電力からパーソナルコンピュータ 1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ 1からの外部電力が使用され、電力単価の高い乾電池 51の消費電力が低減され、かくして乾電池 51の寿命を延ばすことができる。

なお、CPU 53は、パーソナルコンピュータ 1からUSBケーブル 7を介して外部電力の供給を受けたとき、DSP 59の再生処理を停止させることにより、DSP 59からの輻射を低減させ、そ

の結果としてパーソナルコンピュータ 1 を含むシステム全体の輻射を一段と低減させる。

図 4 は、CPU 11 の所定のプログラムの実行等により実現される、パーソナルコンピュータ 1 の機能の構成を説明するブロック図である。コンテンツ管理プログラム 111 は、EMD 選択プログラム 131、チェックイン／チェックアウト管理プログラム 132、暗号方式変換プログラム 135、圧縮方式変換プログラム 136、暗号化プログラム 137、利用条件変換プログラム 139、利用条件管理プログラム 140、認証プログラム 141、復号プログラム 142、PD 用ドライバ 143、購入用プログラム 144 及び購入用プログラム 145 などの複数のプログラムで構成されている。

コンテンツ管理プログラム 111 は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム 111 を読み出しても、インストラクションを特定できないなど）ように構成されている。

EMD 選択プログラム 131 は、コンテンツ管理プログラム 111 がパーソナルコンピュータ 1 にインストールされるとき、コンテンツ管理プログラム 111 には含まれず、後述する EMD の登録の処理において、ネットワーク 2 を介して、EMD 登録サーバ 3 から受信される。EMD 選択プログラム 131 は、EMD サーバ 4-1 乃至 4-3 のいずれかとの接続を選択して、購入用アプリケーション 115、又は購入用プログラム 144 若しくは 142 に、EMD サーバ 4-1 乃至 4-3 のいずれかとの通信（例えば、コンテン

を購入するときの、コンテンツのダウンロードなど)を実行させる。

—チェックイン/チェックアウト管理プログラム132は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトするか、又はポータブルデバイス6-1乃至6-3に記憶されているコンテンツをチェックインする。

チェックイン/チェックアウト管理プログラム132は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新する。

コピー管理プログラム133は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにコピーするか、又はポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114にコピーする。

移動管理プログラム134は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかに移動するか、又はポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114に移動する。

暗号方式変換プログラム135は、ネットワーク2を介して、購

入用アプリケーションプログラム 1 1 5 が EMD サーバ 4-1 から受信したコンテンツの暗号化の方式、購入用プログラム 1 4 4 が EMD サーバ 4-2 から受信したコンテンツの暗号化の方式、又は購入用プログラム 1 4 5 が EMD サーバ 4-3 から受信したコンテンツの暗号化の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1-1 乃至 1 6 1-N に格納されているコンテンツと同一の暗号化の方式に変換する。

また、暗号方式変換プログラム 1 3 5 は、ポータブルデバイス 6-1 又は 6-3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6-1 又は 6-3 が利用可能な暗号化方式に変換する。

圧縮方式変換プログラム 1 3 6 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4-1 から受信したコンテンツの圧縮の方式、購入用プログラム 1 4 4 が EMD サーバ 4-2 から受信したコンテンツの圧縮の方式、又は購入用プログラム 1 4 5 が EMD サーバ 4-3 から受信したコンテンツの圧縮の方式を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1-1 乃至 1 6 1-N に格納されているコンテンツと同一の圧縮の方式に変換する。

また、圧縮方式変換プログラム 1 3 6 は、ポータブルデバイス 6-1 又は 6-3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス 6-1 又は 6-3 が利用可能な圧縮の方式に変換する。

暗号化プログラム 1 3 7 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（暗号化されていない）

を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の暗号化の方式で暗号化する。

圧縮／伸張プログラム 1 3 8 は、例えば CD から読み取られ、録音プログラム 1 1 3 から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース 1 1 4 が記録しているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム 1 3 8 は、符号化されているコンテンツを伸張（復号）する。

利用条件変換プログラム 1 3 9 は、ネットワーク 2 を介して、購入用アプリケーションプログラム 1 1 5 が EMD サーバ 4 - 1 から受信したコンテンツの利用条件を示すデータ（いわゆる、U s a g e R u l e）、購入用プログラム 1 4 4 が EMD サーバ 4 - 2 から受信したコンテンツの利用条件を示すデータ、又は購入用プログラム 1 4 5 が EMD サーバ 4 - 3 から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース 1 1 4 が記録している利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に格納されている利用条件データと同一のフォーマットに変換する。

また、利用条件変換プログラム 1 3 9 は、ポータブルデバイス 6 - 1 又は 6 - 3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス 6 - 1 又は 6 - 3 が利用可能な利用条件のデータに変換する。

利用条件管理プログラム 1 4 0 は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテ

コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 乃至 162-N に格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム 140 は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 乃至 162-N に格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

認証プログラム 141 は、コンテンツ管理プログラム 111 と購入用アプリケーションプログラム 115 との相互認証の処理及びコンテンツ管理プログラム 111 と購入用プログラム 144 との相互認証の処理を実行する。また、認証プログラム 141 は、EMD サーバ 4-1 と購入用アプリケーションプログラム 115 との相互認証の処理、EMD サーバ 4-2 と購入用プログラム 144 との相互認証の処理及び EMD サーバ 4-3 と購入用プログラム 145 との相互認証の処理で利用される認証鍵を記憶している。

認証プログラム 141 が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム 111 がパーソナルコンピュータ 1 にインストールされたとき、認証プログラム 141 に記憶されておらず、表示操作指示プログラム 112 により登録の処理が正常に実行されたとき、EMD 登録サーバ 3 から供給され、認証プログラム 141 に記憶される。

復号プログラム 142 は、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツをパーソナルコンピュータ 1 が再生するとき、コ

ンテンツを復号する。

—PD用ドライバ143は、ポータブルデバイス6-2に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-2から所定のコンテンツをチェックインするとき、ポータブルデバイス6-2にコンテンツ又はポータブルデバイス6-2に所定の処理を実行させるコマンドを供給する。

PD用ドライバ143は、ポータブルデバイス6-1に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-1から所定のコンテンツをチェックインするとき、デバイスドライバ116-1にコンテンツ、又はデバイスドライバ116-1に所定の処理を実行させるコマンドを供給する。

PD用ドライバ143は、ポータブルデバイス6-3に所定のコンテンツをチェックアウトするとき、又はポータブルデバイス6-3から所定のコンテンツをチェックインするとき、デバイスドライバ116-2にコンテンツ、又はデバイスドライバ116-2に所定の処理を実行させるコマンドを供給する。

購入用プログラム144は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム111とともにインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCDに記録されて供給される。購入用プログラム144は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

購入用プログラム144は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで

記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム 1 4 4 を読み出しても、インストラクションを特定できないなど）ように構成されている。

購入用プログラム 1 4 4 は、ネットワーク 2 を介して、EMD サーバ 4 - 2 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4 - 2 からコンテンツを受信する。また、購入用プログラム 1 4 4 は、EMD サーバ 4 - 2 からコンテンツを受信するとき、課金の処理を実行する。

購入用プログラム 1 4 5 は、コンテンツ管理プログラム 1 1 1 とともにインストールされるプログラムであり、ネットワーク 2 を介して、EMD サーバ 4 - 3 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4 - 3 からコンテンツを受信する。また、購入用プログラム 1 4 5 は、EMD サーバ 4 - 3 からコンテンツを受信するとき、課金の処理を実行する。

表示操作指示プログラム 1 1 2 は、フィルタリングデータファイル 1 8 1、表示データファイル 1 8 2、画像ファイル 1 8 3 - 1 乃至 1 8 3 - K、又は履歴データファイル 1 8 4 を基に、ディスプレイ 2 0 に所定のウィンドウの画像を表示させ、キーボード 1 8 又はマウス 1 9 への操作を基に、コンテンツ管理プログラム 1 1 1 にチェックイン又はチェックアウトなどの処理の実行を指示する。

フィルタリングデータファイル 1 8 1 は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD 2 1 に記録されている。

表示データファイル 1 8 2 は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツに対応するデータを格納して、H D D 2 1 に記録されている。

画像ファイル 1 8 3 - 1 乃至 1 8 3 - K は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に対応する画像、又は後述するパッケージに対応する画像を格納して、H D D 2 1 に記録されている。

以下、画像ファイル 1 8 3 - 1 乃至 1 8 3 - K を個々に区別する必要がないとき、単に、画像ファイル 1 8 3 と称する。

履歴データファイル 1 8 4 は、コンテンツデータベース 1 1 4 に記録されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N に格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、H D D 2 1 に記録されている。

表示操作指示プログラム 1 1 2 は、登録の処理のとき、ネットワーク 2 を介して、E M D 登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 1 1 1 の I D を送信するとともに、E M D 登録サーバ 3 から認証用鍵及び E M D 選択プログラム 1 3 1 を受信して、コンテンツ管理プログラム 1 1 1 に認証用鍵及び E M D 選択プログラム 1 3 1 を供給する。

録音プログラム 1 1 3 は、所定のウィンドウの画像を表示させて、キーボード 1 8 又はマウス 1 9 への操作を基に、ドライブ 2 2 に装着された光ディスク 4 2 である C D からコンテンツの録音時間などのデータを読み出す。

録音プログラム 1 1 3 は、CD に記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWW サーバ 5 - 1 又は 5 - 2 に CD に対応するデータ（例えば、アルバム名、又はアーティスト名など）又は CD に記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWW サーバ 5 - 1 又は 5 - 2 から CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを受信する。

録音プログラム 1 1 3 は、受信した CD に対応するデータ又は CD に記録されているコンテンツに対応するデータを、表示操作指示プログラム 1 1 2 に供給する。

また、録音の指示が入力されたとき、録音プログラム 1 1 3 は、ドライブ 2 2 に装着された光ディスク 4 2 である CD からコンテンツを読み出して、コンテンツ管理プログラム 1 1 1 に出力する。

コンテンツデータベース 1 1 4 は、コンテンツ管理プログラム 1 1 1 から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N のいずれかに格納する（HDD 2 1 に記録する）。コンテンツデータベース 1 1 4 は、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N にそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N にそれぞれ対応する利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N のいずれかに格納する（HDD 2 1 に記録する）。

コンテンツデータベース 1 1 4 は、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N 又は利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N をレコードとして記録してもよい。

例えば、コンテンツファイル 1 6 1 - 1 に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 1 6 2 - 1 に格納されている。コンテンツファイル 1 6 1 - N に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 1 6 2 - N に格納されている。

なお、利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N に記録されているデータは、後述する期限データベースに記録されているデータ、又は曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース 1 1 4 は、後述する期限データベース及び曲データベースを包含して、構成されている。

以下、コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N を個々に区別する必要がないとき、単に、コンテンツファイル 1 6 1 と称する。以下、利用条件ファイル 1 6 2 - 1 乃至 1 6 2 - N を個々に区別する必要がないとき、単に、利用条件ファイル 1 6 2 と称する。

購入用アプリケーションプログラム 1 1 5 は、EMD 登録サーバ 3 からネットワーク 2 を介して供給され、又は所定の CD-ROM に記録されて供給される。購入用アプリケーションプログラム 1 1 5 は、ネットワーク 2 を介して、EMD サーバ 4 - 1 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4 - 1 からコンテンツを受信して、コンテンツ管理プログラム 1 1 1 に供給する。また、購入用アプリケーションプログラム 1 1 5 は、EMD サーバ 4 - 1 からコンテンツを受信するとき、課金の処理を実行する。

次に、表示データファイル 8 2 に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N との対応付けについて説明する。

コンテンツファイル 1 6 1 - 1 乃至 1 6 1 - N のいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

オリジナルパッケージは、1 以上のコンテンツが属し、E M D サーバ 4 - 1 乃至 4 - 3 におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚の C D に対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

マイセレクトパッケージは、使用者が任意に選択した 1 以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1 以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

フィルタリングパッケージには、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、E M D サーバ 4 - 1 乃至 4 - 3 又は W W W サーバ 5 - 1 若しくは 5 - 2 などからネットワーク 2 を介して供給され、又は所定の C D に記録されて供給される。使用者は、フィルタリングデータファイル 1 8 1 に格納されているフィルタリングデータを編集することができる。

フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ 1 は、今週の日本のポップス 1 位のコンテンツ乃至今週の日本のポップス 10 位のコンテンツを特定することができる。

フィルタリングデータファイル 181 は、例えば、過去 1 月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ 221（コンテンツ用表示データ 221 に使用者が設定したデータを含む）、又は履歴データ 184 などと、フィルタリングデータとを対応させて選択される。

ドライバ 117 は、コンテンツ管理プログラム 111 などの制御の基に、音声入出力インターフェース 24 を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム 111 に供給するか、若しくはコンテンツ管理プログラム 111 を介してコンテンツデータベース 114 から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム 111 を介してコンテンツデータベース 114 から供給されたコンテンツに対応するアナログ信号を出力する。

図 5 は、表示操作指示プログラム 112 を起動させたとき、操作

指示プログラム 1 1 2 がディスプレイ 2 0 に表示させる表示操作指示ウィンドウの例を示す図である。

表示操作指示ウィンドウには、録音プログラム 1 1 3 を起動させるためのボタン 2 0 1、EMD 選択プログラム 1 3 1 を起動させるためのボタン 2 0 2、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン 2 0 3、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン 2 0 4 等が配置されている。

ボタン 2 0 5 が選択されているとき、フィールド 2 1 1 には、オリジナルパッケージに対応するデータが表示される。ボタン 2 0 6 が選択されているとき、フィールド 2 1 1 には、マイセレクトパッケージに対応するデータが表示される。ボタン 2 0 7 が選択されているとき、フィールド 2 1 1 には、フィルタリングパッケージに対応するデータが表示される。

フィールド 2 1 1 に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

例えば、図 5 においては、パッケージ名称”ファースト”及びアーティスト名”A 太郎”、パッケージ名称”セカンド”及びアーティスト名”A 太郎”などがフィールド 2 1 1 に表示される。

フィールド 2 1 2 には、フィールド 2 1 1 で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド 2 1 2 に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

例えば、図 5 においては、パッケージ名称”セカンド”に対応す

るパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、8分音符の1つがチェックアウト1回に相当し、8分音符が2つでチェックアウト2回を示す）、並びに曲名”北の墓場”及びチェックアウト可能回数（8分音符が1つでチェックアウト1回を示す）などがフィールド212に表示される。

このように、フィールド212に表示されるチェックアウト可能回数としての1つの8分音符は、対応するコンテンツが1回チェックアウトできることを示す。

フィールド212に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が0である。（ただし、パーソナルコンピュータ1はそのコンテンツを再生することができる。））ことを示す。また、フィールド212に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

なお、チェックアウト可能回数は、図5に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等でも表示してもよい。

また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図4の画像ファイル183-1乃至183-Kのいずれかに対応する）を表示させるフィールド208が配置されている。ボタン209は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ4

5に出力させる)とき、クリックされる。

—ボタン205が選択され、フィールド211に、オリジナルパッケージに対応するデータが表示されている場合、フィールド212に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、選択されている曲名に対応する、コンテンツデータベース114に格納されている所定のコンテンツを消去させる。

録音プログラム113が表示させるウィンドウのボタン(後述するボタン255)が選択されて(アクティブにされて)いる場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツの曲名を表示するフィールド213を表示する。

録音プログラム113が表示させるウィンドウのボタンが選択されている場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、コンテンツデータベース114に記録した、CDから読み出したコンテンツを予め指定されているポータブルデバイス6-1乃至6-3のいずれかにチェックアウトさせる。

フィールド213にはコンテンツの曲名に対応させて、フィールド213の最も左に、そのコンテンツがパーソナルコンピュータ1にチェックインできるか否かを示す記号が表示される。例えば、フィールド213の最も左に位置する“○”は、コンテンツの曲名に

対応するコンテンツがパーソナルコンピュータ 1 にチェックインできる（すなわち、パーソナルコンピュータ 1 からチェックアウトされた）ことを示している。フィールド 2 1 3 の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ 1 にチェックインできない（すなわち、パーソナルコンピュータ 1 からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに記憶されているコンテンツが属するパッケージ）の名称を表示するフィールド 2 1 4、フィールド 2 1 3 を閉じるためのボタン 2 1 0 及びチェックイン又はチェックアウトを実行させるボタン 2 1 5 を表示する。

更に、表示操作指示プログラム 1 1 2 が表示操作指示ウィンドウにフィールド 2 1 3 を表示させたとき、表示操作指示プログラム 1 1 2 は、表示操作指示ウィンドウに、フィールド 2 1 2 で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン 2 1 6、フィールド 2 1 3 で選択された曲名に対応するコンテンツのチェックインを設定するボタン 2 1 7、フィールド 2 1 3 に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン 2 1 8 及びチェックイン又はチェックアウトの設定を取り消すボタン 2 1 9 を配置させる。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ 1 は、チェックイン又はチェックアウトの処理を実行しない。

ボタン 2 1 6 乃至 2 1 9 の操作によるチェックイン又はチェックアウトの設定をした後、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン 2 1 5 がクリックされたとき、表示操作指示プログラム 1 1 2 は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム 1 1 1 に、ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかが記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル 1 6 2 に格納されている利用条件のデータを更新させる。

チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム 1 1 2 は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル 1 8 4 に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス 6 - 1 乃至 6 - 3 の名称などから成る。

チェックイン又はチェックアウトの設定の処理は短時間で実行で

きるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

図6は、録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。例えば、WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド251に、“アシンクロナイズド”などのCDのタイトルを表示する。WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド252に、例えば、“クワイ”などのアーティスト名を表示する。

WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド253の曲名を表示する部分に、例えば、“ヒート”，“プラネット”，“ブラック”，“ソウル”などの曲名を表示する。同様に、録音プログラム113は、フィールド253のアーティストを表示する部分に、例えば、“クワイ”などのアーティスト名を表示する。

録音プログラム113が所定のCDの情報を受信した後、録音プログラム113は、HDD21の所定のディレクトリにCDの情報を格納する。

ボタン254などがクリックされて、CDの情報の取得の指示を受けたとき、録音プログラム113は、始めに、HDD21の所定のディレクトリを検索する。録音プログラム113は、そのディレクトリにCDの情報が格納されているとき、図示せぬダイアログボ

ックスを表示して、使用者にディレクトリに格納されているCDの情報を利用するか否かを選択させる。

録音プログラム113が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン256がクリックされたとき、録音プログラム113は、ドライブ22に格納されているCDからコンテンツを読み出して、CDから読み出したコンテンツをCDの情報とともにコンテンツ管理プログラム111に供給する。コンテンツ管理プログラム111の圧縮／伸張プログラム138は、録音プログラム113から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム137は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム139は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

コンテンツ管理プログラム111は、圧縮され、暗号化されたコンテンツを利用条件のデータとともに、コンテンツデータベース114に供給する。

コンテンツデータベース114は、コンテンツ管理プログラム111から受信したコンテンツに対応するコンテンツファイル161及び利用条件ファイル162を生成して、コンテンツファイル161にコンテンツを格納するとともに、利用条件ファイル162に利用条件のデータを格納する。

コンテンツ管理プログラム111は、コンテンツデータベース114にコンテンツ及びコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム113から受信したCDの情報及び利用条件のデータを表示操作指示プログラム112に供給する。

表示操作指示プログラム 1 1 2 は、録音の処理でコンテンツデータベース 1 1 4 に格納されたコンテンツに対応する利用条件のデータ及び CD の情報を基に、表示データファイル 1 8 2 に格納する表示用のデータを生成する。

録音プログラム 1 1 3 が表示させるウィンドウには、更に、CD から読み出したコンテンツをコンテンツデータベース 1 1 4 に記録したとき、自動的に、CD から読み出したコンテンツをポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかにチェックアウトさせるか否かの設定を行うボタン 2 5 5 が配置されている。

例えば、ボタン 2 5 5 がクリックされたとき、録音プログラム 1 1 3 は、ポータブルデバイス 6 - 1 乃至 6 - 3 のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかを選択したとき、パーソナルコンピュータ 1 は、選択されたポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに、自動的に、CD から記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから ”チェックアウトしない” を選択した場合、パーソナルコンピュータ 1 は、CD からコンテンツを記録したとき、チェックアウトしない。

このように、録音プログラム 1 1 3 が表示させるウィンドウのボタン 2 5 5 をアクティブにしておくだけで、CD から読み出したコンテンツがコンテンツデータベース 1 1 4 に記録されたとき、パーソナルコンピュータ 1 は、予め指定されているポータブルデバイス 6 - 1 乃至 6 - 3 のいずれかに、CD から読み出したコンテンツをチェックアウトさせることができる。

次に、図7のフローチャートを参照して、コンテンツ管理プログラム111、表示操作指示プログラム112、録音プログラム113、及びコンテンツデータベース114を実行するCPU11による、ドライブ22に装着されたCDから再生したコンテンツをHDD21に転送し、コピーする場合の処理について説明する。使用者がキーボード18又はマウス19を操作して、インタフェース17を介してCPU11に対してドライブ22に装着されたCD（図示せず）から再生されたコンテンツをHDD21に転送、コピーする指令を入力すると、録音プログラム113は、ステップS11において、インタフェース17を介してディスプレイ20にコピーするコンテンツを選択するための、例えば、図6に示すGUI(Graphical User Interface)を表示させる。

具体的には、例えば、録音プログラム113は、ドライブ22に装着されたCDのTOC(Table Of Contents)を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ20に表示させる。又は、録音プログラム113は、CDに含まれている各コンテンツ毎のISRC(International Standard Recording Code)を読み出し、そのコンテンツの情報を得て、ディスプレイ20に表示させる。あるいはまた、ボタン254がクリックされたとき、録音プログラム113は、ネットワーク2を介してWWWサーバ5-1又は5-2にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド253に表示させる。

使用者は、ディスプレイ20のGUIを利用してキーボード18又はマウス19を操作し、フィールド253に表示されている曲名

に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

次に、ステップS 1 2において、録音プログラム 1 1 3は、利用条件管理プログラム 1 4 0に、H D D 2 1に格納されている期限データベース（図 4に示すコンテンツデータベース 1 1 4の利用条件ファイル 1 6 2 - 1乃至 1 6 2 - Nに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図 8のフローチャートに示されている。

ステップS 3 1において利用条件管理プログラム 1 4 0は、アダプタ 2 6のC P U 3 2と共働して、期限データベース全体のハッシュ値を計算し、ステップS 3 2において、その計算された値と、前回保存しておいたハッシュ値と比較する。

なお、期限データベースにデータが何ら記録されていないとき、利用条件管理プログラム 1 4 0は、ハッシュ値を計算しない。

すなわち、H D D 2 1には、期限データベースが形成されており、この期限データベースには、図 9に示すように、H D D 2 1に記録されているコンテンツ（コンテンツ）を管理する管理情報として、過去に記録されたことのあるコンテンツのI S R Cとコピー日時が対応して記憶されている。この例においては、アイテム 1乃至アイテム 3の3つのアイテムについて、それぞれのI S R Cとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのI S R Cとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS 3 8において、アダプタ 2 6のC P U 3 2により計算され、不揮発性メモリ 3 4に記憶されている。ハッシュ値は、データに対してハッシュ関数を適

用して得られた値である。ハッシュ関数は、一般的に可変長の長いデータを、固定長の短い値にマップする一方向性の関数であり、ハッシュ値同士の衝突が起こりにくい性質を有している。ハッシュ関数の例としては、SHA(Secure Hash Algorithm) , MD(Message Digest) 5 などがある。利用条件管理プログラム 140 は、ステップ S 31 において、CPU 32 が実行したのと同様にハッシュ値を計算する。そして、ステップ S 32 において、利用条件管理プログラム 140 は、CPU 32 に、不揮発性メモリ 34 に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップ S 31 で、いま自分自身が計算したハッシュ値とを比較する。

ステップ S 33 において、利用条件管理プログラム 140 は、ステップ S 31 でいま計算したハッシュ値と、不揮発性メモリ 34 に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム 140 は、ステップ S 34 において、例えば、録音プログラム 113 に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インタフェース 17 を介してディスプレイ 20 に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CD に記録されているコンテンツを再生し、HDD 21 にコピーする処理が禁止される。

ステップ S 31 で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップ S 35 に進み、利用条件管理プログラム 140 は、録音プログラム 113 に、ステップ S 11 で指定されたコピーするコンテンツとして選択されたコンテンツ（選択された

コンテンツ)のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム140は、録音プログラム113に、そのCDのTOCのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

ステップS36において、利用条件管理プログラム140は、ステップS35で取得したISRC(すなわち、選択されたコンテンツ)が期限データベース(図9)に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD21に登録されていないことになるので、ステップS37に進み、利用条件管理プログラム140は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム140は、この現在の日時として、CPU32から転送を受けた、アダプタ26のRTC35が出力する値を利用する。そして、ステップS38において、利用条件管理プログラム140は、その時点における期限データベースのデータを読み出し、アダプタ26のCPU32に転送する。CPU32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

次に、ステップS39において、利用条件管理プログラム140は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS13において、選択されたコンテンツが期限データ

ベースに登録されているか否かの判定を行うときに用いられる。

ステップS 3 6において、選択されたコンテンツのI S R Cが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、H D D 2 1に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップS 4 0に進み、利用条件管理プログラム1 4 0は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ2 6のR T C 3 5が出力した現在の日時）が4 8時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に4 8時間以上経過している場合には、H D D 2 1に、少なくとも一度は記録したことがあるが、既に、その時から4 8時間以上経過しているので、そのコンテンツを再度コピーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場合には、H D D 2 1へのコピーが許容される。そこで、ステップS 4 1に進み、利用条件管理プログラム1 4 0は、期限データベースの日時を、過去の登録日時から現在の日時（R T C 3 5の出力する日時）に変更させる。そして、ステップS 3 8に戻り、利用条件管理プログラム1 4 0は、再び、期限データベース全体のハッシュ値をC P U 3 2に計算させ、不揮発性メモリ3 4に保存させるとともに、ステップS 3 9において、そのコンテンツに対して未登録のフラグを設定する。

一方、ステップS 4 0において、現在時刻が登録日時より、まだ4 8時間以上経過していないと判定された場合、その選択されたコンテンツのH D D 2 1へのコピーが禁止される。そこで、この場合には、ステップS 4 2に進み、利用条件管理プログラム1 4 0は、

その選択されたコンテンツに対応して登録済みのフラグを設定する。ステップS 40の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売又は配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップS 40においては、判定の基準は48時間以上の経過としたが、48時間に限らず、例えば、12時間乃至168時間のいずれかの時間であればよい。

以上のようにして、期限データベースチェック処理により、選択されたコンテンツがHDD 21に登録されているか否かを表すフラグが設定される。

図7に戻り、ステップS 13においてコピー管理プログラム133は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップS 14に進み、コピー管理プログラム133は、録音プログラム113に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ20に表示させる。これにより、使用者は、そのコンテンツをHDD 21にコピーすることができない理由を知ることができる。

ステップS 13において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップS 15に進み、録音プログラム113は、ドライブ22を制御し、そこに装着されているCDからコンテンツを読み出させる。このコンテンツには、

図10に示すように、所定の位置にウォーターマークコードが挿入されている。録音プログラム113は、ステップS16において、コンテンツに含まれているウォーターマークコードを抽出し、そのウォーターマークコードがコピー禁止を表しているのか否かをステップS17において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップS18に進み、録音プログラム113は、録音プログラム113に例えば、「コピーは禁止されています」のようなメッセージをインタフェース17を介してディスプレイ20に表示させ、コピー処理を終了させる。

これに対して、ステップS17において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップS19に進み、録音プログラム113は、コンテンツを、圧縮／伸張プログラム138に、例えば、A T R A C (Adaptive Transform Acoustic Coding) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップS20において、録音プログラム113は、暗号化プログラム137に、予め設定され、メモリ13に記憶されている暗号鍵を用いて、例えば、D E S (Data Encryption Standard) 方式、F E A L (Fast Encipherment Algorithm) 方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ26のCPU32により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ1だけではなく、それに付随して装着されたハードウェアとしてのアダプタ26のCPU32と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

次に、ステップS 2 1において、録音プログラム 1 1 3は、暗号化されたデータを、コンテンツデータベース 1 1 4に転送し、1つのファイル（コンテンツファイル 1 6 1として）としてファイル名を付けてHDD 2 1に保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

この保存処理と、上記した圧縮符号化処理及び暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

さらに、ステップS 2 2において、録音プログラム 1 1 3は、暗号化プログラム 1 3 7に、予め定められている不揮発性メモリ 3 4に記憶されている保存用鍵を使って、上述したDES方式、FEAL方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、HDD 2 1の曲データベース（図4に示すコンテンツデータベース 1 1 4の利用条件ファイル 1 6 2 - 1乃至 1 6 2 - Nに対応する）に保存する。

ステップS 2 3において、録音プログラム 1 1 3は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者がGUIを介して入力した曲名の情報の要素を組にしてHDD 2 1の曲データベースに登録する（利用条件ファイル 1 6 2 - 1乃至 1 6 2 - Nとして記録する）。そして、ステップS 2 4において、録音プログラム 1 1 3は、CPU 3 2に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ 3 4に保存させる。

このようにして、例えば、図11に示すような曲データベースが、HDD 2 1上に登録される。この例においては、アイテム1乃至ア

アイテム 3 のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ及びコピー条件（S C M S）が記録されている。

例えば、S D M I (Secure Digital Music Initiative) が規定する方式では、C D からコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、3 回に設定される。

C D から H D D 2 1 にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ 1 が故障して、H D D 2 1 に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、H D D 2 1 に記録することができる。

また、例えば、ネットワーク 2 を介して H D D 2 1 に記録されている期限データベースの内容を共有することもできる。

以上においては、I S R C に対応して複製された日時が記憶されている場合を例として説明したが、コンテンツや C D を識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組合せなど）を利用することもできる。

次に、図 1 2 乃至図 1 4 のフローチャートを参照して、表示操作指示プログラム 1 1 2 及びコンテンツ管理プログラム 1 1 1 を実行する C P U 1 1 及びメインプログラムを実行する C P U 5 2 による、

HDD 21 からポータブルデバイス 6 のフラッシュメモリ 61 (例えば、メモリースティック (商標)) に、コンテンツを移動する処理及びチェックアウトの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップ S 51 において、移動管理プログラム 134 は、利用条件管理プログラム 140 に、曲データベース全体のハッシュ値を計算させ、ステップ S 52 で、前回 CPU 32 に計算させ、不揮発性メモリ 34 に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム 134 は、ステップ S 53 に進み、表示操作指示プログラム 112 に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ 20 に表示させた後、処理を終了させる。この場合の処理は、図 8 のステップ S 31 乃至ステップ S 34 の処理と同様の処理である。この場合においては、HDD 21 からポータブルデバイス 6 へのコンテンツの移動が実行されないことになる。

次に、ステップ S 54 において、移動管理プログラム 134 は、HDD 21 に形成されている曲データベース (コンテンツデータベース 114 に含まれる) から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム 112 に、選択のための GUI としてディスプレイ 20 に表示させる。使用者は、この選択のための GUI に基づいて、HDD 21 からポータブルデバイス 6 へ移動させるコンテンツを、図 5 のフィールド 212 に表示される曲名、ボタン 216 などをクリックして選択する。次に、ステップ S 55 において、移動管理プログラム 134 は、ステップ S 54 で選択された選択されたコンテンツの再生条件、コピー条件、再生時

課金条件などを調べる。この処理の詳細は、図 15 のフローチャートを参照して後述する。

次に、ステップ S 5 6 において、パーソナルコンピュータ 1 の認証プログラム 1 4 1 とポータブルデバイス 6 の CPU 5 3 との間において、相互認証処理が行われ、通信用鍵が共有される。

例えば、ポータブルデバイス 6 のフラッシュメモリ 6 1 (又は、EEPROM 6 8) には、マスター鍵 KM が予め記憶されており、パーソナルコンピュータ 1 の RAM 1 3 (又は、HDD 2 1 の所定のファイル) には、個別鍵 KP と ID が予め記憶されているものとする。CPU 5 3 は、認証プログラム 1 4 1 から、RAM 1 3 に予め記憶されている ID の供給を受け、その ID と自分自身が有するマスター鍵 KM にハッシュ関数を適用して、RAM 1 3 に記憶されているパーソナルコンピュータ 1 の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ 1 とポータブルデバイス 6 の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

あるいはまた、パーソナルコンピュータ 1 の RAM 1 3 に ID とマスター鍵 KMP を予め記憶させておくとともに、ポータブルデバイス 6 のフラッシュメモリ 6 1 にもポータブルデバイス 6 の ID とマスター鍵 KMM を記憶させておく。そして、それぞれの ID とマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきた ID とマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

なお、認証の方法としては、例えば、IOS(International Org

anization for Standardization) 9 7 9 8 - 2 を利用することができる。

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップ S 5 7 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図 7 のステップ S 2 0 の処理で暗号化されている）を HDD 2 1 から読み出す。ステップ S 5 8 において、移動管理プログラム 1 3 4 は、ステップ S 5 7 で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップ S 1 9 の処理）、暗号化方式（ステップ S 2 0 の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス 6 のものに変換する処理を実行する。この変換処理の詳細は、図 1 7 のフローチャートを参照して後述する。

ステップ S 5 9 において、移動管理プログラム 1 3 4 は、PD 用ドライバ 1 4 3 に、ステップ S 5 8 で変換したコンテンツを、USB ポート 2 3 を介してポータブルデバイス 6 に転送させる。ステップ S 6 0 において、ポータブルデバイス 6 の CPU 5 3 は、USB コネクタ 5 6 を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ 6 1 に記憶させる。

ステップ S 6 1 において、移動管理プログラム 1 3 4 は、さらに、利用条件変換プログラム 1 3 9 に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス 6 が管理している形式に変換する。ステップ S 6 2 において、移動管理プログラム 1 3 4 は、さ

らに、利用条件変換プログラム 139 に、選択されたコンテンツの曲データベース中に登録されているコピー条件中の S C M S 情報を、ポータブルデバイス 6 の管理する形式に変換させる。そして、ステップ S 63 において、移動管理プログラム 134 は、P D 用ドライバ 143 に、ステップ S 61 で変換した再生条件と、ステップ S 62 で変換した S C M S 情報を、ポータブルデバイス 6 に転送させる。ポータブルデバイス 6 の C P U 53 は、転送を受けた再生条件と S C M S 情報を、フラッシュメモリ 61 に保存する。

ステップ S 64 において、移動管理プログラム 134 はまた、P D 用ドライバ 143 に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、C P U 11 が曲データベース中で扱っている形式のまま、ポータブルデバイス 6 に転送させ、フラッシュメモリ 61 に保存させる。

ステップ S 65 において、移動管理プログラム 134 は、コンテンツデータベース 114 に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップ S 66 において、復号プログラム 142 に、その暗号鍵を R A M 13 に保存されている保存用鍵で復号させ、暗号化プログラム 137 に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム 134 は、P D 用ドライバ 143 に、ポータブルデバイス 6 へ転送させる。

ポータブルデバイス 6 の C P U 53 は、ステップ S 67 で、パーソナルコンピュータ 1 から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ 61

に保存する。

—CPU 53は、暗号鍵の保存が完了すると、ステップS68において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1の移動管理プログラム134は、ポータブルデバイス6からこの通知を受けると、ステップS69において、コンテンツデータベース114に、そのコンテンツに対応するコンテンツファイル161を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル162）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS70において、移動管理プログラム134は、アダプタ26のCPU32に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。このハッシュ値が、上述したステップS52において、前回保存しておいたハッシュ値として用いられることになる。

次に、パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理は、図12乃至図14のパーソナルコンピュータ1からポータブルデバイス6へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ1においてチェックイン／チェックアウト管理プログラム132により実行され、図14のステップS69において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（又は

チェックアウトできる回数)を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

次に、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 1 2 のステップ S 5 5 における選択されたコンテンツの再生条件などのチェック処理について図 1 5 のフローチャートを参照して説明する。ステップ S 8 1 において、移動管理プログラム 1 3 4 は、コンテンツデータベース 1 1 4 に、曲データベースから、各種の条件を読み出させる。移動管理プログラム 1 3 4 は、ステップ S 8 2 において、ステップ S 8 1 で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既に過ぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップ S 8 3 に進み、移動管理プログラム 1 3 4 は、表示操作指示プログラム 1 1 2 に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ 2 0 に表示させ、処理を終了させる。ステップ S 8 2 において、コピー回数がコピー制限回数を過ぎていると判定された場合、ステップ S 8 4 に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ 2 6 の RTC 3 5 より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ 1 の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム 1 3 4 は、この現在日時を CPU 3 2 から提供を受けて、ステップ S 8 4 の判断を自ら行うか、又は、ステップ S 8 1 で、曲データベースから読み出した再生条件をアダプタ 2 6 の

CPU 32に供給し、CPU 32に、ステップS 84の判定処理を実行させる。

現在日時が再生終了日時を過ぎている場合、ステップS 85に進み、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツをHDD 21から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップS 86において、移動管理プログラム134は、CPU 32に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ34に保存させる。以後、処理は終了される。したがって、この場合、コンテンツの移動が実行されない。

ステップS 84において、現在日時が、再生終了日時を過ぎていると判定された場合、ステップS 87に進み、移動管理プログラム134は、その選択されたコンテンツの再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム134は、ステップS 88において、PD用ドライバ143に、ポータブルデバイス6と通信させ、ポータブルデバイス6に課金機能が存在するか否かを判定する。ポータブルデバイス6に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス6に転送する訳にはいかないので、ステップS 89において、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ20に表示させ、コンテンツの移動処理を終了させる。

ステップS 87において再生時課金条件が登録されていないと判

定された場合、又は、ステップS 8 8において、ポータブルデバイス6に課金機能が存在すると判定された場合、ステップS 9 0に進み、移動管理プログラム1 3 4は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS 9 1に進み、移動管理プログラム1 3 4は、ポータブルデバイス6に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス6が、その再生条件を守る機能を有していない場合には、ステップS 9 2に進み、移動管理プログラム1 3 4は、表示操作指示プログラム1 1 2に、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ2 0に表示させ、処理を終了させる。

ステップS 9 0において、再生条件が登録されていないと判定された場合、又はステップS 9 1において、ポータブルデバイス6が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図1 2のステップS 5 6に戻る。

図1 6は、ポータブルデバイス6が管理している（守ることが可能な）再生条件の例を表している。図1 6に示す再生情報は、例えば、EEPROM 6 8に記憶されている。この例においては、アイテム1乃至アイテム3の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム2についてのみ登録されており、アイテム1とアイテム3については登録されていない。したがって、アイテム2のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム1又はアイテム3のコンテンツが選択されたコンテン

ツとされた場合、再生回数の条件は守ることができないことになる。

次に、図17のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、図12のステップS58におけるフォーマット変換処理の詳細について説明する。ステップS101において、移動管理プログラム134は、コンテンツデータベース114に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップS102において、移動管理プログラム134は、相手先の機器（今の場合、ポータブルデバイス6）に設定することが可能な条件を調べる。すなわち、移動管理プログラム134は、ポータブルデバイス6のCPU53に設定可能な条件を問い合わせ、その回答を得る。ステップS103において移動管理プログラム134は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップS102で調べた条件に基づいて決定する。

ステップS104において、移動管理プログラム134は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、コンテンツをポータブルデバイス6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス6が守ることができないので、そのようなポータブルデバイス6には、コンテンツを移動することが禁止されるのである。

ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、移動管理プログラム134は、利用条件変換プログラム139に、その条件を相手先の機能フォー

マットの条件（例えば、ポータブルデバイス 6 に転送する際、ヘッドに格納される条件）に変換させる。そして、ステップ S 1 0 7 において、移動管理プログラム 1 3 4 は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス 6 は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

次に、図 1 8 乃至図 2 0 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 及びメインプログラムを実行する CPU 5 3 による、HDD 2 1 からポータブルデバイス 6 にコンテンツをコピーする場合の処理について説明する。この図 1 8 乃至図 2 0 のステップ S 1 1 1 乃至ステップ S 1 2 7 の処理は、コピー管理プログラム 1 3 3 により実行され、図 1 2 乃至図 1 4 の HDD 2 1 からポータブルデバイス 6 へコンテンツを移動させる場合のステップ S 5 1 乃至ステップ S 6 7 の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス 6 と、パーソナルコンピュータ 1 との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ 1 の HDD 2 1 からポータブルデバイス 6 のフラッシュメモリ 6 1 に転送され、保存される。その後、ステップ S 1 2 8 において、コピー管理プログラム 1 3 3 は、曲データベースのコピー回数カウンタを 1 だけインクリメントする。そして、ステップ S 1 2 9 において、コピー管理プログラム 1 3 3 は、CPU 3 2 に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ 3 4 に保存させる。

次に、図 2 1 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 及びメインプログラムを実行する CPU 5 3 による、ポータブルデバイス 6 から HDD 2 1 にコンテンツを移動する処理及びチェックインの処理について説明する。

始めに、コンテンツの移動の処理について説明する。ステップ S 1 6 1 において、移動管理プログラム 1 3 4 は、ポータブルデバイス 6 の CPU 5 3 に対してフラッシュメモリ 6 1 に記憶されているコンテンツの情報の読み出しを要求する。CPU 5 3 は、この要求に対応して、フラッシュメモリ 6 1 に記憶されているコンテンツの情報をパーソナルコンピュータ 1 に送信する。移動管理プログラム 1 3 4 は、この情報に基づいて、ディスプレイ 2 0 に、フラッシュメモリ 6 1 に記憶されているコンテンツを選択するための GUI を表示させる。使用者は、キーボード 1 8 又はマウス 1 9 を操作して、その GUI に基づいて、ポータブルデバイス 6 から HDD 2 1 (コンテンツデータベース 1 1 4) に移動させるコンテンツを指定する。

ステップ S 1 6 2 において、移動管理プログラム 1 3 4 は、認証プログラム 1 4 1 に、CPU 5 3 との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図 1 2 のステップ S 5 6 における場合と同様の処理である。

次に、ステップ S 1 6 3 において、CPU 5 3 は、フラッシュメモリ 6 1 に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ 1 に転送する。移動管理プログラム 1 3 4 は、ステップ S 1 6 4 において、ポータブルデバイス 6 から転送されてきたコンテンツを、1 つのファイルとしてファイル名を付けて、コンテンツデータベース 1 1 4 (HDD 2 1) に保

存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

ステップS 1 6 5において、CPU 5 3は、フラッシュメモリ 6 1に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ 1に転送する。この暗号鍵は、例えば、図 1 4のステップS 6 7の処理でフラッシュメモリ 6 1に保存されていたものである。

ステップS 1 6 6において、移動管理プログラム 1 3 4は、ポータブルデバイス 6から暗号鍵の転送を受けると、復号プログラム 1 4 2に、それを通信用鍵で復号させ、暗号化プログラム 1 3 7に、自分自身の保存用鍵で暗号化させる。ステップS 1 6 7で、移動管理プログラム 1 3 4は、コンテンツデータベース 1 1 4に、ステップS 1 6 4で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がGUIを介して入力した曲名、ステップS 1 6 6で暗号化した暗号鍵などを、HDD 2 1の曲データベースに登録させる。そして、ステップS 1 6 8において、移動管理プログラム 1 3 4は、利用条件管理プログラム 1 4 0に、その曲データベース全体のハッシュ値をCPU 3 2に計算させ、不揮発性メモリ 3 4に保存させる。

ステップS 1 6 9において、移動管理プログラム 1 3 4は、ポータブルデバイス 6に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU 5 3は、パーソナルコンピュータ 1から、そのコンテンツの削除が要求されてきたとき、ステッ

ブ S 1 7 0 において、フラッシュメモリ 6 1 に記憶されているそのコンテンツを削除する。

次に、ポータブルデバイス 6 からパーソナルコンピュータ 1 にコンテンツをチェックインする処理について説明する。ポータブルデバイス 6 からパーソナルコンピュータ 1 にコンテンツをチェックインする処理は、図 2 1 のポータブルデバイス 6 からパーソナルコンピュータ 1 へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ 1 においてチェックイン／チェックアウト管理プログラム 1 3 2 により実行され、図 2 1 のステップ S 1 6 2 乃至 S 1 6 6 の処理が省略される。また、パーソナルコンピュータ 1 は、図 2 1 のステップ S 1 6 7 において、曲データベースに記録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、ステップ S 1 7 0 の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

なお、ポータブルデバイス 6 のフラッシュメモリ 6 1 がメモリカードとして着脱可能であるとき、パーソナルコンピュータ 1 は、チェックインの処理において、図 2 1 のステップ S 1 6 2 の相互認証の処理を実行する。

次に、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 及びメインプログラムを実行する CPU 5 3 による、ポータブルデバイス 6 から HDD 2 1 へコンテンツをコピーする場合の処理について、図 2 2 のフローチャートを参照して説明する。この図 2 2 に示すステップ S 1 8 1 乃至ステップ S 1 8 8 の処理は、図 2 1 のポー

タブルデバイス 6 から HDD 2 1 へコンテンツを移動させる場合の処理におけるステップ S 1 6 1 乃至ステップ S 1 6 8 の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム 1 3 3 により実行され、図 2 1 のステップ S 1 6 9 , S 1 7 0 の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

次に、図 2 3 のフローチャートを参照して、EMD サーバ 4 及びコンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、EMD サーバ 4 から転送を受けたコンテンツを HDD 2 1 にコピーする処理について説明する。ステップ S 2 0 1 において、購入用プログラム 1 4 4 は、図 5 に示すボタン 2 0 2 がクリックされて、使用者から EMD サーバ 4 へのアクセスが指令されたとき、通信部 2 5 を制御し、ネットワーク 2 を介して EMD サーバ 4 にアクセスさせる。EMD サーバ 4 は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク 2 を介してパーソナルコンピュータ 1 に転送する。購入用プログラム 1 4 4 は、通信部 2 5 を介して、この情報を取得したとき、表示操作指示プログラム 1 1 2 に、それをインタフェース 1 7 を介してディスプレイ 2 0 に表示させる。使用者は、ディスプレイ 2 0 に表示された GUI を利用して、ステップ S 2 0 2 において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク 2 を介して EMD サーバ 4 に転送される。ステップ S 2 0 3 において、購入用プログラム 1 4 4 は、EMD サーバ 4 との間において、ネットワーク 2 を介して相互認証処理を実行し、通信用鍵を共有する。

パーソナルコンピュータ 1 と EMD サーバ 4 との間で行われる相互認証処理は、例えば、ISO 9798-3 で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ 1 は、自分自身の秘密鍵と EMD サーバ 4 の公開鍵を予め有しており、EMD サーバ 4 は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ 1 の公開鍵は、EMD サーバ 4 から転送したり、あるいはパーソナルコンピュータ 1 に予め配布されている証明書(certificate) をパーソナルコンピュータ 1 から EMD サーバ 4 に転送し、その証明書を EMD サーバ 4 が確認し、公開鍵を得るようにしてもよい。さらに、ステップ S 204 において、購入用プログラム 144 は、EMD サーバ 4 との間において課金に関する処理を実行する。この課金の処理の詳細は、図 24 のフローチャートを参照して後述する。

次に、ステップ S 205 において、EMD サーバ 4 は、パーソナルコンピュータ 1 に対して、ステップ S 202 で指定された、暗号化されているコンテンツをネットワーク 2 を介してパーソナルコンピュータ 1 に転送する。このとき、時刻情報も適宜転送される。ステップ S 206 において、購入用プログラム 144 は、コンテンツデータベース 114 に、転送を受けたコンテンツにファイル名を付けて HDD 21 に 1 つのコンテンツファイル 161 として保存させる。ステップ S 207 において、EMD サーバ 4 は、さらに、そのコンテンツの暗号鍵をステップ S 203 でパーソナルコンピュータ 1 と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ 1 へ転送する。

購入用プログラム 144 は、ステップ S 208 において、復号プ

プログラム 142 に、EMD サーバ 4 より転送を受けた暗号鍵を単独で、又はアダプタ 26 の CPU 32 と共同して通信用鍵を用いて復号させ、暗号化プログラム 137 に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップ S209 において、購入用プログラム 144 は、コンテンツデータベース 114 に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD 21 の曲データベースに登録させる。さらに、ステップ S210 において、購入用プログラム 144 は、その曲データベース全体のハッシュ値を CPU 32 に計算させ、不揮発性メモリ 34 に保存させる。

なお、ステップ S205 において EMD サーバ 4 は、コンテンツとともに、時刻データをパーソナルコンピュータ 1 に送信する。この時刻データは、パーソナルコンピュータ 1 からアダプタ 26 に転送される。アダプタ 26 の CPU 32 は、パーソナルコンピュータ 1 より転送されてきた時刻データを受信すると、ステップ S211 において、RTC 35 の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ 26 の RTC 35 の時刻情報を修正するようにしたので、アダプタ 26 を常に正しい時刻情報を保持することが可能となる。

次に、図 24 のフローチャートを参照して、EMD サーバ 4 及びコンテンツ管理プログラム 111 を実行する CPU 11 による、図 23 のステップ S204 における課金に関する処理の詳細について説明する。ステップ S221 において、購入用プログラム 144 は、ステップ S201 で EMD サーバ 4 から伝送されてきた価格情報の

中から、ステップS 2 0 2で指定された選択されたコンテンツの価格情報を読み取り、これをH D D 2 1上の課金ログに書き込む。図 2 5は、このような課金ログの例を表している。この例においては、使用者は、アイテム1乃至アイテム3を、E M Dサーバ4からコピーしており、アイテム1とアイテム2の領域は5 0円とされ、アイテム3の料金は6 0円とされている。その時点における課金ログのハッシュ値も、C P U 3 2により計算され、不揮発性メモリ3 4に登録されている。

次に、ステップS 2 2 2において、購入用プログラム1 4 4は、ステップS 2 2 1で書き込んだ課金ログをH D D 2 1から読み出し、これをネットワーク2を介してE M Dサーバ4に転送する。E M Dサーバ4は、ステップS 2 2 3において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、E M Dサーバ4は、内蔵するデータベースに、パーソナルコンピュータ1の使用者から伝送されてきた課金ログを追加更新する。そして、ステップS 2 2 4において、E M Dサーバ4は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS 2 2 5に進み、E M Dサーバ4は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップS 2 2 6において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS 2 2 4において、決裁は直ちには行われないと判定された場合、ステップS 2 2 5とS 2 2 6の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

次に、図2 6と図2 7のフローチャートを参照して、コンテンツ

管理プログラム 111 を実行する CPU 11 による、音声入出力インタフェース 24 の IEC 60958 端子 24 a から入力された、図示せぬ CD プレーヤなどからの再生されたコンテンツを、HDD 21 にコピーする場合の処理について説明する。ステップ S 241 において、使用者は、CD プレーヤの IEC 60958 出力端子を、パーソナルコンピュータ 1 の音声入出力インタフェース 24 の IEC 60958 端子 24 a に接続する。ステップ S 242 において、使用者は、キーボード 18 又はマウス 19 を操作し、CD プレーヤからコピーするコンテンツの曲名（又は、コンテンツに対応する番号）を入力する。そして、ステップ S 243 において使用者は、CD プレーヤのボタンを操作し、CD プレーヤの再生を開始させる。CD プレーヤとパーソナルコンピュータ 1 との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ 1 のキーボード 18 又はマウス 19 を介して再生開始指令を入力することで、CD プレーヤに CD の再生を開始させることも可能である。

CD プレーヤにおいて、CD の再生が開始されると、ステップ S 244 において、CD プレーヤから出力されたコンテンツが、IEC 60958 端子 24 a を介してパーソナルコンピュータ 1 に転送されてくる。ステップ S 245 において、コピー管理プログラム 133 は、IEC 60958 端子 24 a を介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。この SCMS データには、コピー禁止、コピー 1 回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップ S 246 において、CPU 11 は、SCMS データがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ス

テップS 2 4 7に進み、コピー管理プログラム1 3 3は、表示操作指示プログラム1 1 2に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ2 0に表示させ、コピー処理を終了する。すなわち、この場合には、H D D 2 1へのコピーが禁止される。

コピー管理プログラム1 3 3は、ステップS 2 4 6において、ステップS 2 4 5で読み取ったS C M S情報がコピー禁止を表していないと判定した場合、ステップS 2 4 8に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップS 2 4 9において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS 2 4 7に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

ステップS 2 4 9において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS 2 5 0に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップS 2 5 1, S 2 5 2の処理で、処理が終了される。この処理は、図7のステップS 1 3, S 1 4の処理と同様の処理である。

選択されたコンテンツがまだH D D 2 1に登録されていないコンテンツであれば、ステップS 2 5 3乃至S 2 5 8で、その登録処理が実行される。このステップS 2 5 3乃至ステップS 2 5 8の処理は、ステップS 2 5 7において、I E C 6 0 9 5 8端子2 4 aから供給されてくるS C M S情報も曲データベースに登録される点を除き、図7のステップS 1 9乃至ステップS 2 4の処理と同様の処理

であるので、その説明は省略する。

次に、図28と図29のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、コンテンツをHDD21からIEC60958端子24aに出力（再生）する場合の処理について説明する。ステップS271乃至ステップS273において、図18のステップS111乃至S113における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS274に進み、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、HDD21の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、ディスプレイ20に表示させる。使用者は、その表示を見て、キーボード18又はマウス19を適宜操作して、再生出力するコンテンツを選択する。ステップS275において、表示操作指示プログラム112は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図30のフローチャートを参照して後述する。

次に、ステップS276において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、ステップS274において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム142に保存用鍵で復号させる。ステップS277において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介し

て、コンテンツデータベース 114 に、選択されたコンテンツの S CMS 情報を曲データベースから読み出させ、IEC 60958 端子 24 a から出力する S CMS 情報を、S CMS システムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は 1 だけインクリメントされ、新たな S CMS 情報とされる。ステップ S 278 において、表示操作指示プログラム 112 はさらに、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、選択されたコンテンツの I SRC を曲データベースから読み出させる。

次に、ステップ S 279 において、表示操作指示プログラム 112 は、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツを HDD 21 から読み出させる。表示操作指示プログラム 112 はさらに、コンテンツ管理プログラム 111 を介して、コンテンツデータベース 114 に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム 142 に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム 138 は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップ S 280 において、表示操作指示プログラム 112 は、ドライバ 117 に、ステップ S 279 で、復号したデジタルデータであるコンテンツを、ステップ S 277 で決定した S CMS 情報、並びにステップ S 278 で読み出した I SRC 情報とともに、IEC 60958 の規定に従って、IEC 60958 端子 24 a から出力させる。さらにまた、表示操作指示プログ

ラム 1 1 2 は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インタフェース 2 4 のアナログ出力端子から出力させる。

ステップ S 2 8 1 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、曲データベース中の再生回数カウンタの値を 1 だけインクリメントさせる。そして、ステップ S 2 8 2 において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップ S 2 8 3 に進み、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、対応する料金を課金ログに書き込ませ、ステップ S 2 8 4 において、表示操作指示プログラム 1 1 2 は、利用条件管理プログラム 1 4 0 に、曲データベース全体のハッシュ値を CPU 3 2 に計算させ、不揮発性メモリ 3 4 に記憶させる。ステップ S 2 8 2 において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップ S 2 8 3 とステップ S 2 8 4 の処理はスキップされる。

次に、図 3 0 のフローチャートを参照して、コンテンツ管理プログラム 1 1 1 を実行する CPU 1 1 による、図 2 8 のステップ S 2 7 5 の再生条件等のチェック処理の詳細について説明する。ステップ S 3 0 1 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介して、コンテンツデータベース 1 1 4 に、曲データベースの各種条件を読み出させる。ステップ S 3 0 2 において利用条件管理プログラム 1 4 0 は、読み出した条件のうち、

再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS 3 0 3に進み、コンテンツ管理プログラム1 1 1を介して、コンテンツデータベース1 1 4に、選択されたコンテンツをH D D 2 1から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップS 3 0 4において、表示操作指示プログラム1 1 2はさらに、利用条件管理プログラム1 4 0に、曲データベースの新たなハッシュ値をC P U 3 2に計算させ、そのハッシュ値を不揮発性メモリ3 4に保存させる。この場合、再生出力は禁止される。

ステップS 3 0 2において、再生回数が制限回数を過ぎていないと判定された場合、ステップS 3 0 5に進み、利用条件管理プログラム1 4 0 2は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップS 3 0 3において、選択されたコンテンツをH D D 2 1から削除させるとともに、曲データベースからも削除させる。そして、ステップS 3 0 4において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

ステップS 3 0 5において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップS 3 0 6に進み、C P U 3 2は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS 3 0 7に進み、表示操作指示プログラム1 1 2は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ2 0に表示させる。ステップS 3 0 6において、再生時課金条件

が付加されていないと判定された場合、ステップS 3 0 7の処理はスキップされる。

次に、図3 1と図3 2のフローチャートを参照して、コンテンツ管理プログラム1 1 1を実行するCPU 1 1及びメインプログラムを実行するCPU 5 3による、HDD 2 1からポータブルデバイス6経由でコンテンツを出力（再生）する場合の処理について説明する。ステップS 3 2 1乃至ステップS 3 2 5において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図2 8のステップS 2 7 1乃至ステップS 2 7 5の処理と同様の処理であるので、その説明は省略する。

ステップS 3 2 6において、ポータブルデバイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS 3 2 7において、表示操作指示プログラム1 1 2は、ポータブルデバイス6に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップS 3 2 8において、表示操作指示プログラム1 1 2は、ステップS 3 2 4で、コンテンツ管理プログラム1 1 1を介してコンテンツデータベース1 1 4に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD 2 1から読み出させる。表示操作指示プログラム1 1 2は、ステップS 3 2 9において、コンテンツ管理プログラム1 1 1に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス6の方式のものに変換する処理を実行させる。そして、ステップS 3 3 0において、表示操作指示プログラム1 1 2

は、暗号化プログラム 1 3 7 に、ステップ S 3 2 9 において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス 6 に転送する。

ステップ S 3 3 1 において、ポータブルデバイス 6 の CPU 5 3 は、ステップ S 3 2 7 において、パーソナルコンピュータ 1 から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップ S 3 3 2 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 に、曲データベースの再生回数カウンタを 1 だけインクリメントさせる。さらに、ステップ S 3 3 3 において、表示操作指示プログラム 1 1 2 は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップ S 3 3 4 において、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 に、その料金を課金ログに書き込ませ、ステップ S 3 3 5 において、CPU 3 2 に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップ S 3 3 4、ステップ S 3 3 5 の処理はスキップされる。

本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU 1 1 を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

さらに、上述したように、CPU 1 1 の機能の一部は、ハードウェアとしてのアダプタ 2 6 に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高める

ことが可能となっている。

例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ 26 の不揮発性メモリ 34 に保存される。すなわち、図 8 のステップ S 32, S 33 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 34 に記憶されているものとされる。これにより、例えば、他の記録媒体にコピー又は移動させる前に、HDD 21 に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD 21 から、そこに保存されているコンテンツを他の記録媒体にコピー又は移動した後、HDD 21 にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピー又は移動ができてしまうようなことが防止される。

例えば、図 33 に示すように、HDD 21 にコンテンツ A, B が保存されている場合、不揮発性メモリ 34 には、コンテンツ A とコンテンツ B の情報に対応するハッシュ値が保存されている。この状態において、HDD 21 のコンテンツ A, B を含む記録データの一部又は全部を他の記録媒体 271 にバックアップしたとする。その後、HDD 21 に保存されているコンテンツ A とコンテンツ B のうち、コンテンツ A を他の記録媒体 272 に移動させた場合、その時点において、HDD 21 に記録されているコンテンツは、コンテンツ B だけとなるので、不揮発性メモリ 34 のハッシュ値も、コンテンツ B に対応するハッシュ値に変更される。

したがって、その後、記録媒体 271 にバックアップしておいた

HDD 21のコンテンツA、Bを含む記録データの一部又は全部をHDD 21にリストアして、HDD 21に、再びコンテンツAとコンテンツBを保存させたとしても、不揮発性メモリ34には、コンテンツBの情報から演算されたハッシュ値が記憶されており、コンテンツAとコンテンツBの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 21に記憶されているコンテンツAとコンテンツBに基づくハッシュ値が、不揮発性メモリ34に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 21に保存されているコンテンツAとコンテンツBの利用が制限されてしまうことになる。

さらに、上述したように、アダプタ26は、RTC 35を内蔵しており、このRTC 35の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ1が管理するものではなく、RTC 35が出力するものが利用される。したがって、使用者が、パーソナルコンピュータ1の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

また、アダプタ26は、暗号化されて転送されてきたプログラムをROM 36に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図34のフローチャートを参照して説明する。

すなわち、パーソナルコンピュータ1は、アダプタ26に対して、所定の処理を実行させたいとき、ステップS351において、アダ

アダプタ 26 に実行させるべきプログラムを R A M 1 3 に予め記憶されている暗号鍵を用いて暗号化してアダプタ 26 に転送する。アダプタ 26 の R O M 3 6 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。C P U 3 2 は、この R O M 3 6 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 3 5 2 において復号する。そして、ステップ S 3 1 3 において、C P U 3 2 は、復号したプログラムを R A M 3 3 に展開し、ステップ S 3 5 4 において、そのプログラムを実行する。

例えば、上述したように、パーソナルコンピュータ 1 の C P U 1 1 は、H D D 2 1 の曲データベースのハッシュ値をアダプタ 26 に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ 26 の C P U 3 2 に転送する。C P U 3 2 は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ 3 4 に記憶させる。あるいは、そのハッシュ値を、C P U 3 2 は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ 1 の C P U 1 1 に転送する。

図 3 5 は、アダプタ 26 の内部のより具体的な構成を表している。アダプタ 26 は、半導体 I C として形成される。アダプタ 26 は、図 2 に示したインタフェース 3 1、C P U 3 2、R A M 3 3、不揮発性メモリ 3 4、R T C 3 5、R O M 3 6 以外に、R A M 3 3 に対する書き込みと読み出しを制御する R A M コントローラ 3 0 1、並びに論理回路 3 0 2 を有している。論理回路 3 0 2 は、例えば、暗

号化されているコンテンツを解読した後、解読したデータをアダプタ 26 から直接出力するような場合の処理のために用いられる。

これらのインタフェース 31 乃至 ROM 36、RAM コントローラ 301 並びに論理回路 302 は、半導体 IC 内に一体的に組み込まれ、外部からは分解できないように構成されている。

水晶振動子 311 は、アダプタ 26 が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路 312 は、RTC 35 を動作させるための発振回路である。バッテリー 313 は、発振回路 312、不揮発性メモリ 34 及び RTC 35 に対してバックアップ用の電力を供給している。アダプタ 26 のその他の回路には、パーソナルコンピュータ 1 の電源供給回路 321 からの電力が供給されている。

不揮発性メモリ 34 は、書き込み消去可能な ROM で構成することも可能であるが、バッテリー 313 からのバックアップ電源でバックアップされる RAM で構成する場合には、例えば、図 36A 及び図 36B に示すように、不揮発性メモリ 34 の上に保護アルミニウム層 351 を形成し、さらに、その保護アルミニウム層 351 と同一平面上となるように、不揮発性メモリ 34 にバッテリー 313 からの電力を供給する電源パターン 352 を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ 34 を改竄すべく、保護アルミニウム層 351 を削除しようとする、同一平面上の電源パターン 352 も削除されてしまい、不揮発性メモリ 34 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

さらに、図 3 7 に示すように、不揮発性メモリ 3 4 に対するデータの書き込み又は読み出しのための配線 4 0 1 - 1 乃至 4 0 1 - 3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 4 0 1 - 3 からデータを読み出すためには、上方の配線 4 0 1 - 1, 4 0 1 - 2 を除去しなければならず、複数の配線 4 0 1 - 1, 4 0 1 - 2, 4 0 1 - 3 から同時にデータを読み取ることができなくなる。

さらにまた、不揮発性メモリ 3 4 は、配線 4 0 1 - 1 乃至 4 0 1 - 3 を冗長に形成するようにすることができる。例えば、不揮発性メモリ 3 4 内部に形成される配線 4 0 1 - 1 乃至 4 0 1 - 3 が不揮発性メモリ 3 4 を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにすることで、配線 4 0 1 - 1 乃至 4 0 1 - 3 の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

不揮発性メモリ 3 4 からデータを読み出すために設計されている専用の回路（半導体 I C としてのアダプタ 2 6 に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ 3 4 が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ 3 4 に記憶されているデータを読み出すべく、プローブを配線 4 0 1 - 1 乃至 4 0 1 - 3 に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

以上においては、記録媒体として、ポータブルデバイス 6 を用い

る場合を例として説明したが、本発明は、その他の記録媒体にデータを移転又はコピーする場合にも応用することが可能である。

また、コンテンツは、曲のデータ又は音声データなどの楽音データ以外に、画像データ、その他のデータとすることもできる。

以上のように、本発明によれば、次のような効果を奏することができる。

(1) HDD 21 に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上で HDD 21 に記録するようにしたので、HDD 21 に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

(2) 所定の曲を 1 回コピーしたとき、一定時間（上記例の場合、48 時間）の間、その曲をコピーすることができないようにするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

さらにデータベースを更新するたびに、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

(3) 外部の装置にコンテンツを渡したら、HDD 21 上のコンテンツを消去するようにしたので、HDD 21 内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

(4) HDD 21 内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD 21 の内容をムーブ

の直前にバックアップし、ムーブ直後にバックアップしたデータをHDD 21にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ26に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

なお、アダプタ26が実行する処理は、セキュアなプログラムでCPU11が実行するようにしてもよい。この場合において、例えば、同一な値を有する保存用鍵は、保存用鍵が必要になった時点で、コンテンツ管理プログラム111により生成される。同様に、ハッシュ値は、コンテンツ管理プログラム111により隠蔽されて保存

される。

—また、アダプタ 2 6 が実行する処理が、セキュアなプログラムで CPU 1 1 により実行されるとき、パーソナルコンピュータ 1 は、アダプタ 2 6 の RTC 3 5 が供給する現在時刻に代えて、ネットワーク 2 に接続されている特定のサーバ（例えば、EMD 登録サーバ 3）から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ 1 は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、又は、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図 2 に示すように、磁気ディスク 4 1（フロッピーディスクを含む）、光ディスク 4 2（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク 4 3（MD(Mini-Disc)を含む）、若しくは半導体メモリ 4 4 などよりなるパッケージメディア、又は、プログラムが一時的若しくは永続的に格納される ROM 1 2 や、HDD 2 1 などにより構成される。プログラム格

納媒体へのプログラムの格納は、必要に応じて通信部 25 などのインタフェースを介して、ローカルエリアネットワーク又はインターネットなどのネットワーク 2、デジタル衛星放送といった、有線又は無線の通信媒体を利用して行われる。

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

以上の如く、本発明に係る情報処理装置、情報処理方法及びプログラム格納媒体によれば、蓄積手段に対するコンテンツデータの蓄積又は読み出しを、ハードウェアに設けられた実行手段の実行結果に基づいて、ソフトウェアからなる制御手段により制御するようにしたので、ソフトウェアを解析し、改竄することで、不正にデータを複製することを確実に防止することが可能となる。

— 請求の範囲

1. コンテンツデータを蓄積する蓄積手段と、

前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、

前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含み、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御することを特徴とする情報処理装置。

2. 前記蓄積手段は、蓄積している前記コンテンツデータを管理する管理情報も蓄積しており、

前記制御手段は、前記実行手段に、前記管理情報に基づいて所定の演算を実行させることを特徴とする請求の範囲第1項に記載の情報処理装置。

3. 前記制御手段は、CPUであり、

前記蓄積手段は、ハードディスクであり、

前記実行手段は、前記制御手段としてのCPUとは別の半導体ICに組み込まれたCPUであることを特徴とする請求項1に記載の情報処理装置。

4. コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化さ

れているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の情報処理方法において、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含む

ことを特徴とする情報処理方法。

5. コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の前記制御手段に、

前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含むことを特徴とするコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

6. コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

前記蓄積手段に蓄積するデータを所定の方式で圧縮する圧縮手段と、

前記蓄積手段に蓄積するデータを所定の方式で暗号化する暗号化手段と、

前記圧縮手段により圧縮され、かつ前記暗号化手段により暗号化された前記データの、前記蓄積手段に対する蓄積又は読み出しを制

御する制御手段とを含むことを特徴とする情報処理装置。

7. 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを同一の方式で圧縮又は暗号化することを特徴とする請求の範囲第6項に記載の情報処理装置。

8. 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを同一の方式で圧縮又は暗号化するとともに、前記蓄積手段から読み出された前記データを、予め定められている所定の装置に出力するときに、前記予め定められている共通の圧縮方式又は暗号化方式とすることを特徴とする請求の範囲第6項に記載の情報処理装置。

9. データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含むことを特徴とする情報処理方法。

10. データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

1 1. コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

前記蓄積手段に蓄積されたデータの管理情報を保持する保持手段と、

前記保持手段に保持されている前記管理情報に基づき所定の演算を行う演算手段と、

前記演算手段の演算結果を記憶する記憶手段と、

前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結果と比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの利用を制御する制御手段を含むことを特徴とする情報処理装置。

1 2. 前記演算手段は、前記管理情報にハッシュ関数を適用して前記演算を行うことを特徴とする請求の範囲第 1 1 項に記載の情報処理装置。

1 3. 前記データは音楽データであり、前記管理情報は前記音楽データを識別する識別情報を含むことを特徴とする請求の範囲第 1 1 項に記載の情報処理装置。

1 4. データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果と比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含むことを特徴とする情報処理方法。

15. データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果と比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

16. 他の装置との間でデータを授受する授受手段と、
所定の固定鍵と保存用鍵を保持する保持手段と、

前記他の装置との間でデータを授受するとき、前記保持手段に保持されている前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証手段と、

前記通信用鍵を前記保存用鍵で暗号化する暗号化手段と、

前記授受手段により受信された、前記通信用鍵で暗号化されているデータを、前記暗号化手段により暗号化された前記通信用鍵と対応させて蓄積する蓄積手段とを含むことを特徴とする情報処理装置。

17. 前記蓄積手段に蓄積されている前記通信用鍵を、前記保存用鍵を用いて復号する暗号鍵復号手段と、

前記暗号鍵復号手段により復号された前記通信用鍵を用いて、前記蓄積手段に蓄積されているデータを復号するデータ復号手段とをさらに含むことを特徴とする請求の範囲対16項に記載の情報処理装置。

18. 他の装置との間でデータを授受する授受ステップと、
所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とする情報処理方法。

19. 他の装置との間でデータを授受する授受ステップと、
—所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

20. データを蓄積する蓄積手段と、

前記蓄積手段に蓄積されている前記データの利用時の条件を保持する保持手段と、

前記蓄積手段に蓄積されている前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記蓄積手段に蓄積されている前記データを前記保持手段に保持されている前記データの利用時の条件とともに前記他の装置に移転する移転手段とを含むことを特徴とする情報処理装置。

21. 前記データの利用時の条件は、再生制限条件、再生時課金条件又はコピー制限条件を含むこと請求の範囲対20項に記載の情報処理装置。

22. データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含むことを特徴とする情報処理方法。

23. データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

補正書の請求の範囲

[2000年7月31日(31.07.00)国際事務局受理：出願当初の請求の範囲4-23は補正された；新しい請求の範囲24-35が加えられた；他の請求の範囲は変更なし。(15頁)]

1. コンテンツデータを蓄積する蓄積手段と、

前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、

前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含み、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御することを特徴とする情報処理装置。

2. 前記蓄積手段は、蓄積している前記コンテンツデータを管理する管理情報も蓄積しており、

前記制御手段は、前記実行手段に、前記管理情報に基づいて所定の演算を実行させることを特徴とする請求の範囲第1項に記載の情報処理装置。

3. 前記制御手段は、CPUであり、

前記蓄積手段は、ハードディスクであり、

前記実行手段は、前記制御手段としてのCPUとは別の半導体ICに組み込まれたCPUであることを特徴とする請求の範囲第1項に記載の情報処理装置。

4. (補正後) コンテンツデータ及び該コンテンツデータに付随したコンテンツ管理情報を蓄積するストレージ媒体と、

前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出

しを制御するソフトウェアからなる処理コントローラと、

前記処理コントローラから暗号化されているプログラムが供給され、該プログラムを復号して実行し、実行の結果を前記処理コントローラに供給する、前記処理コントローラとは独立した半導体チップに設けられたプログラム実行コントローラとを含み、

前記処理コントローラは、前記プログラム実行コントローラの実行結果に基づいて、前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御し、

前記プログラム実行コントローラは、その内部処理が上記半導体チップの外部からは確認不能とされ、上記コンテンツ管理情報に対する改竄確認のための演算を行うことを特徴とする情報処理装置。

5. (補正後) コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の情報処理方法において、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含む

ことを特徴とする情報処理方法。

6. (補正後) コンテンツデータ及び該コンテンツデータに付随したコンテンツ管理情報を蓄積するストレージ媒体と、

前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる処理コントローラと、

前記処理コントローラから暗号化されているプログラムが供給され、該プログラムを復号して実行し、実行の結果を前記処理コントローラに供給する、前記処理コントローラとは独立した半導体チップに設けられたプログラム実行コントローラとを含み情報処理装置の情報処理方法において、

前記処理コントローラは、前記プログラム実行コントローラの実行結果に基づいて、前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御し、

前記プログラム実行コントローラは、その内部処理が上記半導体チップの外部からは確認不能とされ、上記コンテンツ管理情報に対する改竄確認のための演算を行うことを特徴とする情報処理方法。

7. (補正後) コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の前記制御手段に、

前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含むことを特徴とするコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

8. (補正後) コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

前記蓄積手段に蓄積するデータを所定の方式で圧縮する圧縮手段と、

前記蓄積手段に蓄積するデータを所定の方式で暗号化する暗号化手段と、

前記圧縮手段により圧縮され、かつ前記暗号化手段により暗号化された前記データの、前記蓄積手段に対する蓄積又は読み出しを制御する制御手段とを含むことを特徴とする情報処理装置。

9. (補正後) 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを同一の方式で圧縮又は暗号化することを特徴とする請求の範囲第8項に記載の情報処理装置。

10. (補正後) 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを異なる方式で圧縮又は暗号化するとともに、前記蓄積手段から読み出された前記データを、予め定められている所定の装置に出力するときに、前記予め定められている共通の圧縮方式又は暗号化方式とすることを特徴とする請求の範囲第8項に記載の情報処理装置。

11. (補正後) コンテンツデータを所定の記録媒体或いはサーバから入力するインターフェースと、

前記インターフェースにより入力されたコンテンツデータを蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積するコンテンツデータを所定の方式で圧縮する圧縮プログラムと、

前記ストレージ媒体に蓄積するコンテンツデータを所定の方式で暗号化する暗号化プログラムと、

前記圧縮プログラムにより圧縮され、かつ前記暗号化プログラムにより暗号化された前記コンテンツデータの、前記ストレージ媒体に対する蓄積又は読み出しを制御するコントローラを含み、

前記圧縮プログラムと前記暗号化プログラムは、前記インターフェースにより入力された異なる方式のコンテンツデータを、同一の方式或いは異なる方式でそれぞれ圧縮又は暗号化して上記ストレージ媒体に蓄積するとともに、異なる方式で圧縮又は暗号化された前記コンテンツデータを前記ストレージ媒体から読み出して、所定のポータブルデバイスに出力するときは、所定の共通の圧縮方式又は暗号化方式となるように変換処理を行うことを特徴とする情報処理装置。

12. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含むことを特徴とする情報処理方法。

13. (補正後) コンテンツデータを所定の記録媒体或いはサーバから入力する入力ステップと、

前記入力ステップの処理で入力されたコンテンツデータをストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積したコンテンツデータを所定の方式で圧縮する圧縮ステップと、

前記圧縮ステップの処理で蓄積したコンテンツデータを所定の方

式で暗号化する暗号化ステップと、

一前記圧縮ステップの処理で圧縮され、かつ前記暗号化ステップの処理で暗号化された前記コンテンツデータの、前記ストレージ媒体に対する蓄積又は読み出しを制御する制御ステップとを含み、

前記圧縮ステップと暗号化ステップは、前記入力ステップの処理で入力された異なる方式のコンテンツデータを、同一の方式或いは異なる方式でそれぞれ圧縮又は暗号化して上記ストレージ媒体に蓄積するとともに、異なる方式で圧縮又は暗号化された前記コンテンツデータを前記ストレージ媒体から読み出して、所定のポータブルデバイスに出力するときは、所定の共通の圧縮方式又は暗号化方式となるように変換処理を行うことを特徴とする情報処理方法。

14. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

15. (補正後) コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

前記蓄積手段に蓄積されたデータの管理情報を保持する保持手段と、

前記保持手段に保持されている前記管理情報に基づき所定の演算を行う演算手段と、

前記演算手段の演算結果を記憶する記憶手段と、

前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結果とを比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの利用を制御する制御手段を含むことを特徴とする情報処理装置。

16. (補正後) 前記演算手段は、前記管理情報にハッシュ関数を適用して前記演算を行うことを特徴とする請求の範囲第15項に記載の情報処理装置。

17. (補正後) 前記データは音楽データであり、前記管理情報は前記音楽データを識別する識別情報を含むことを特徴とする請求の範囲第15項に記載の情報処理装置。

18. (補正後) コンテンツデータ及び該コンテンツデータにかかる識別情報を入力するインターフェースと、

前記インターフェースにより入力されたコンテンツデータを蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積されたコンテンツデータの識別情報を利用条件ファイルとして保持する第1のメモリと、

前記第1のメモリに保持されている前記識別情報にハッシュ関数を適用して演算を行う管理プログラムと、

前記管理プログラムの演算結果を記憶する第2のメモリと、

前記管理プログラムの演算結果と、前記第2のメモリに記憶され

ている過去の前記演算結果とを比較し、一致していない場合は前記ストレージ媒体に蓄積されている前記コンテンツデータのコピー或いは移動に関する処理を禁止するコントローラとを含むことを特徴とする情報処理装置。

19. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含むことを特徴とする情報処理方法。

20. (補正後) コンテンツデータ及び該コンテンツデータにかかる識別情報を入力する入力ステップと、

前記入力ステップにより入力されたコンテンツデータをストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたコンテンツデータの識別情報を利用条件ファイルとして保持する保持ステップと、

前記保持ステップの処理で保持された前記識別情報にハッシュ関数を適用して演算を行う演算ステップと、

前記演算ステップの処理での演算結果を記憶する記憶ステップと、

前記演算ステップの処理での演算結果と、前記記憶ステップの処理で記憶されている過去の前記演算結果とを比較し、一致していない場合は前記ストレージ媒体に上記蓄積ステップの処理で蓄積された前記コンテンツデータのコピー或いは移動に関する処理を禁止する制御ステップとを含むことを特徴とする情報処理方法。

21. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

22. (補正後) 他の装置との間でデータを授受する授受手段と、

所定の固定鍵と保存用鍵を保持する保持手段と、

前記他の装置との間でデータを授受するとき、前記保持手段に保持されている前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証手段と、

前記通信用鍵を前記保存用鍵で暗号化する暗号化手段と、

前記授受手段により受信された、前記通信用鍵で暗号化されているデータを、前記暗号化手段により暗号化された前記通信用鍵と対応させて蓄積する蓄積手段とを含むことを特徴とする情報処理装置。

23. (補正後) 前記蓄積手段に蓄積されている前記通信用鍵を、前記保存用鍵を用いて復号する暗号鍵復号手段と、

前記暗号化鍵復号手段により復号された前記通信用鍵を用いて、前記蓄積手段に蓄積されているデータを復号するデータ復号手段とをさらに含むことを特徴とする請求の範囲第22項に記載の情報処理装置。

24. (追加) 接続されたポータブルデバイス或いはサーバとの間でデータを授受するインターフェースと、

所定のマスター鍵及び保存用鍵を保持するメモリと、

前記ポータブルデバイス或いはサーバとの間で上記データを授受するとき、前記メモリに保持されている前記マスター鍵を利用して、前記ポータブルデバイス或いはサーバとの間で相互認証処理を行い、通信用鍵を生成する認証プログラムと、

上記ポータブルデバイス或いはサーバから送信されたコンテンツデータを暗号化した暗号鍵を前記通信用鍵で復号し、前記保存用鍵で暗号化する暗号復号プログラムと、

前記インターフェースにより受信された、前記通信用鍵で暗号化されている上記コンテンツデータを、前記暗号復号プログラムにより復号され、上記保存用鍵で暗号化された暗号鍵と対応させて蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積されている前記暗号鍵を、前記保存用鍵を用いて復号する暗号鍵復号プログラムと、

前記暗号鍵復号プログラムにより復号された前記暗号鍵を用いて、前記ストレージ媒体に蓄積されているコンテンツデータを復号するデータ復号プログラムとを含むことを特徴とする情報処理装置。

25. (追加) 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とする情報処理方法。

26. (追加) 接続されたポータブルデバイス或いはサーバとの間でデータを授受する授受ステップと、

所定のマスター鍵及び保存用鍵を保持する保持ステップと、

前記ポータブルデバイス或いはサーバとの間で上記データを授受するとき、前記保持ステップの処理で保持した前記マスター鍵を利用して、前記ポータブルデバイス或いはサーバとの間で相互認証処理を行い、通信用鍵を生成する認証ステップと、

上記ポータブルデバイス或いはサーバから送信されたコンテンツデータを暗号化した暗号鍵を前記通信用鍵で復号し、前記保存用鍵で暗号化する暗号復号ステップと、

前記授受ステップにより受信された、前記通信用鍵で暗号化され

ている上記コンテンツデータを、前記暗号復号ステップの処理により復号され、上記保存用鍵で暗号化された暗号鍵と対応させてストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理でストレージ媒体に蓄積した前記暗号鍵を、前記保存用鍵を用いて復号する暗号鍵復号ステップと、

前記暗号鍵復号ステップの処理により復号された前記暗号鍵を用いて、前記ストレージ媒体に蓄積されているコンテンツデータを復号するデータ復号ステップとを含むことを特徴とする情報処理方法。

27. (追加) 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

28. (追加) データを蓄積する蓄積手段と、

前記蓄積手段に蓄積されている前記データの利用時の条件を保持する保持手段と、

前記蓄積手段に蓄積されている前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否

かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記蓄積手段に蓄積されている前記データを前記保持手段に保持されている前記データの利用時の条件とともに前記他の装置に移転する移転手段とを含むことを特徴とする情報処理装置。

29. (追加) 前記データの利用時の条件は、再生制限条件、再生時課金条件又はコピー制限条件を含むことを特徴とする請求の範囲第28項に記載の情報処理装置。

30. (追加) コンテンツデータを蓄積するストレージデバイスと、

前記ストレージデバイスに蓄積されている前記コンテンツデータの利用条件データを保持するメモリと、

前記ストレージデバイスに蓄積されている前記コンテンツデータをポータブルデバイスに移転するとき、前記ポータブルデバイスが、前記利用条件データを充足できるか否かを判定する移転管理プログラムとを有し、

前記移転管理プログラムの判定結果において、前記ポータブルデバイスが、前記利用条件データを充足できないと判断された場合は、前記ストレージデバイスに蓄積されている前記コンテンツデータを前記ポータブルデバイスに移転することを禁止することを特徴とする情報処理装置。

31. (追加) 前記移転は、コピー、移動或いはチェックアウトを含み、前記利用条件データは、再生制限条件、再生時課金条件、又はコピー制限条件を含むことを特徴とする請求の範囲第30項に記載の情報処理装置。

32. (追加) データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含むことを特徴とする情報処理方法。

33. (追加) コンテンツデータをストレージデバイスに蓄積する蓄積ステップと、

前記ストレージデバイスに蓄積されている前記コンテンツデータの利用条件データをメモリに保持する保持ステップと、

前記ストレージデバイスに蓄積されている前記コンテンツデータをポータブルデバイスに移転するとき、前記ポータブルデバイスが、前記利用条件データを充足できるか否かを判定する判定ステップと、

前記判定ステップの判定結果において、前記ポータブルデバイスが、前記利用条件データを充足できないと判断された場合は、前記ストレージデバイスに蓄積されている前記コンテンツデータを前記ポータブルデバイスに移転することを禁止する禁止ステップとを有することを特徴とする情報処理方法。

34. (追加) 前記移転は、コピー、移動或いはチェックアウトを含み、前記利用条件データは、再生制限条件、再生時課金条件、又はコピー制限条件を含むことを特徴とする請求の範囲第33項に

記載の情報処理方法。

3-5. (追加) データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

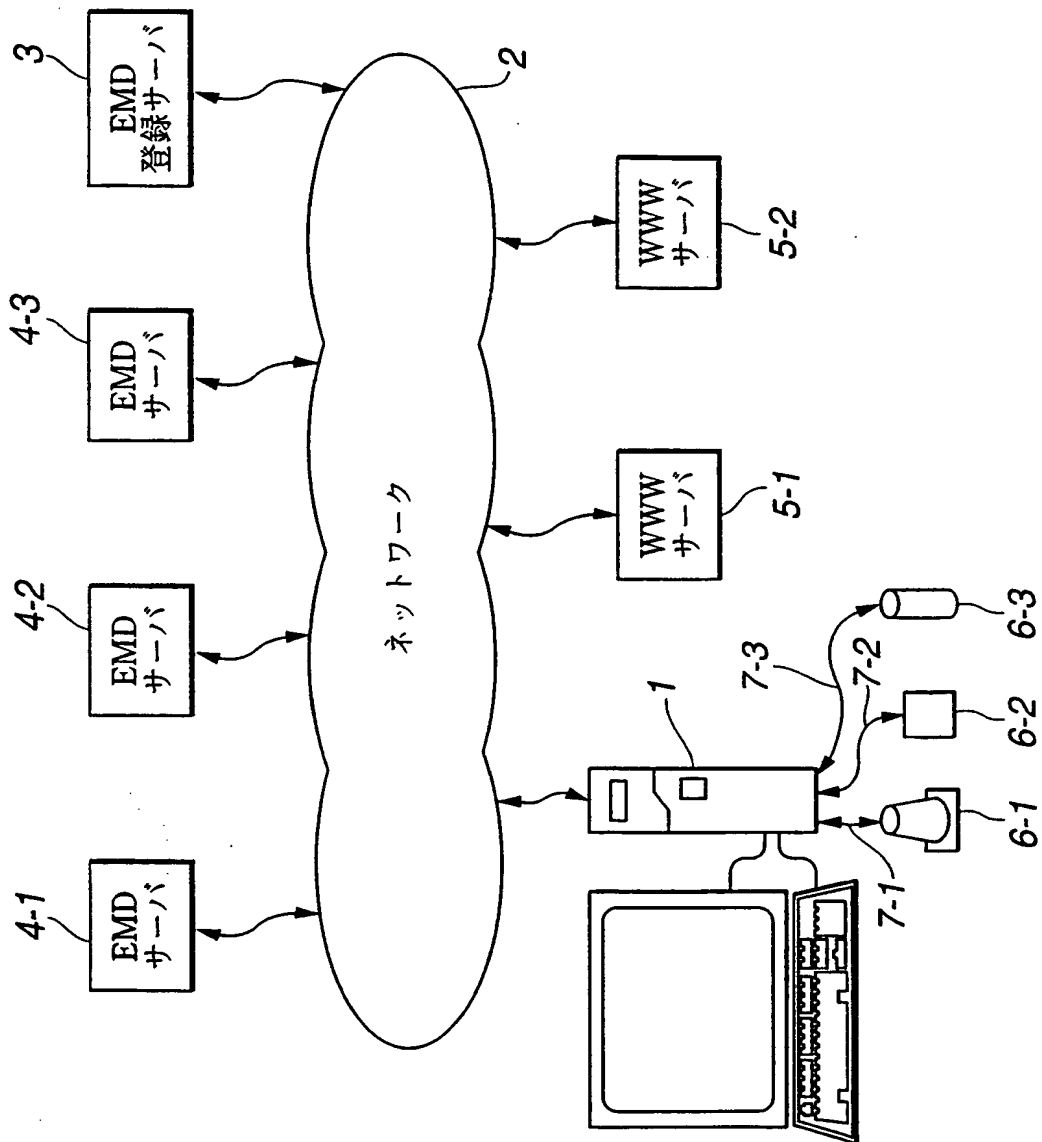


FIG.1

This Page Blank (uspto)

2/36

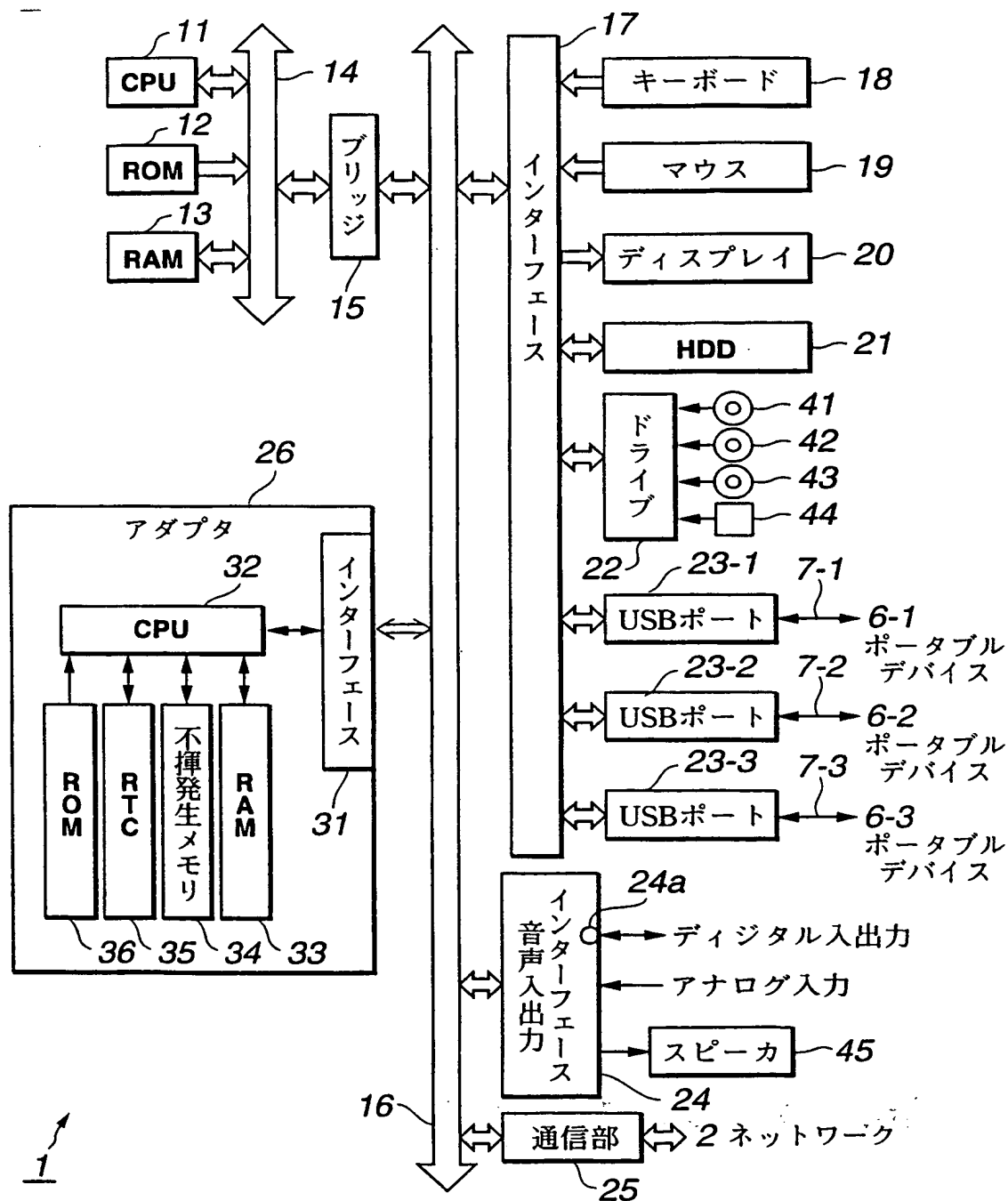


FIG.2

This Page Blank (uspto)

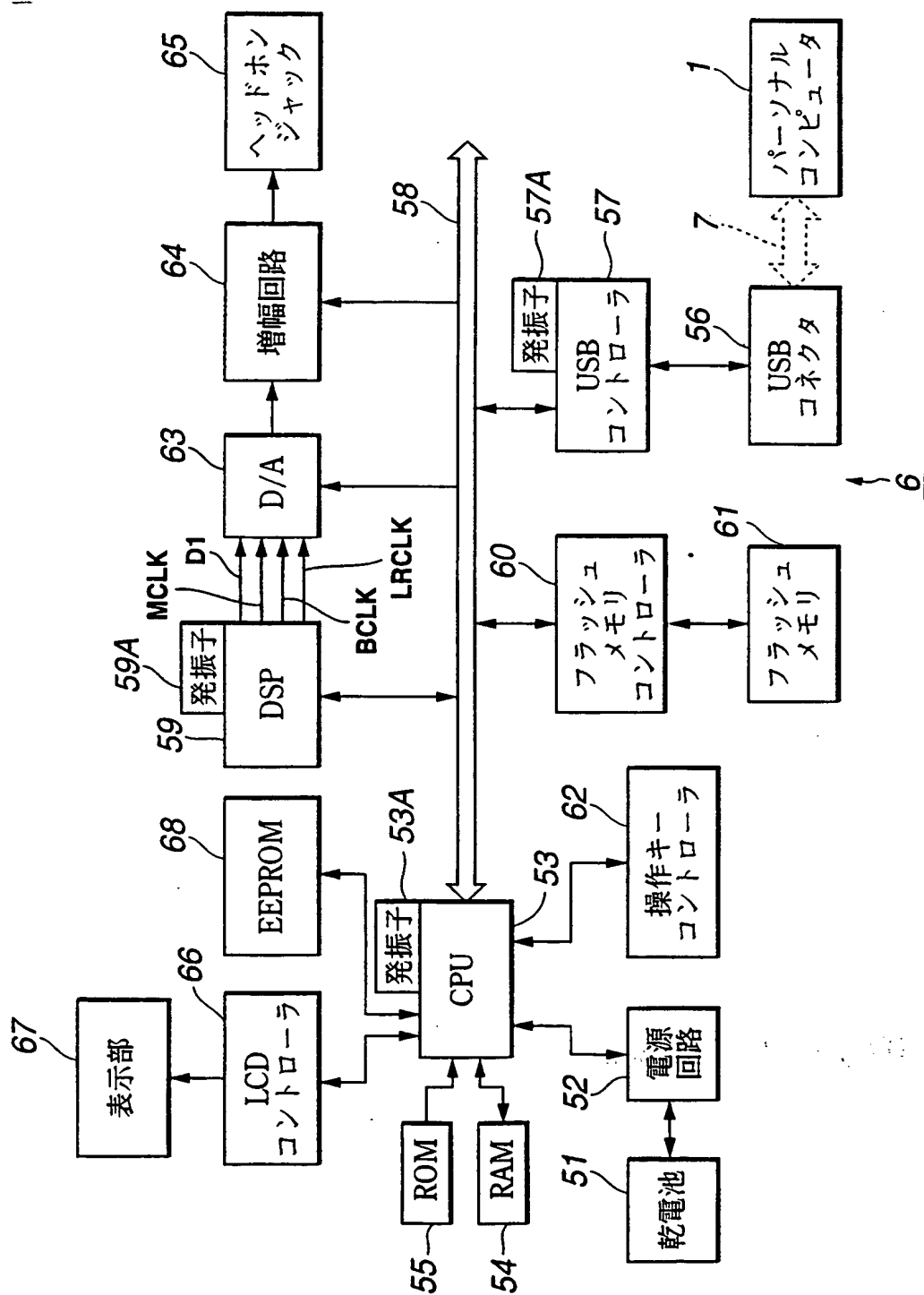


FIG.3

This Page Blank (uspto)

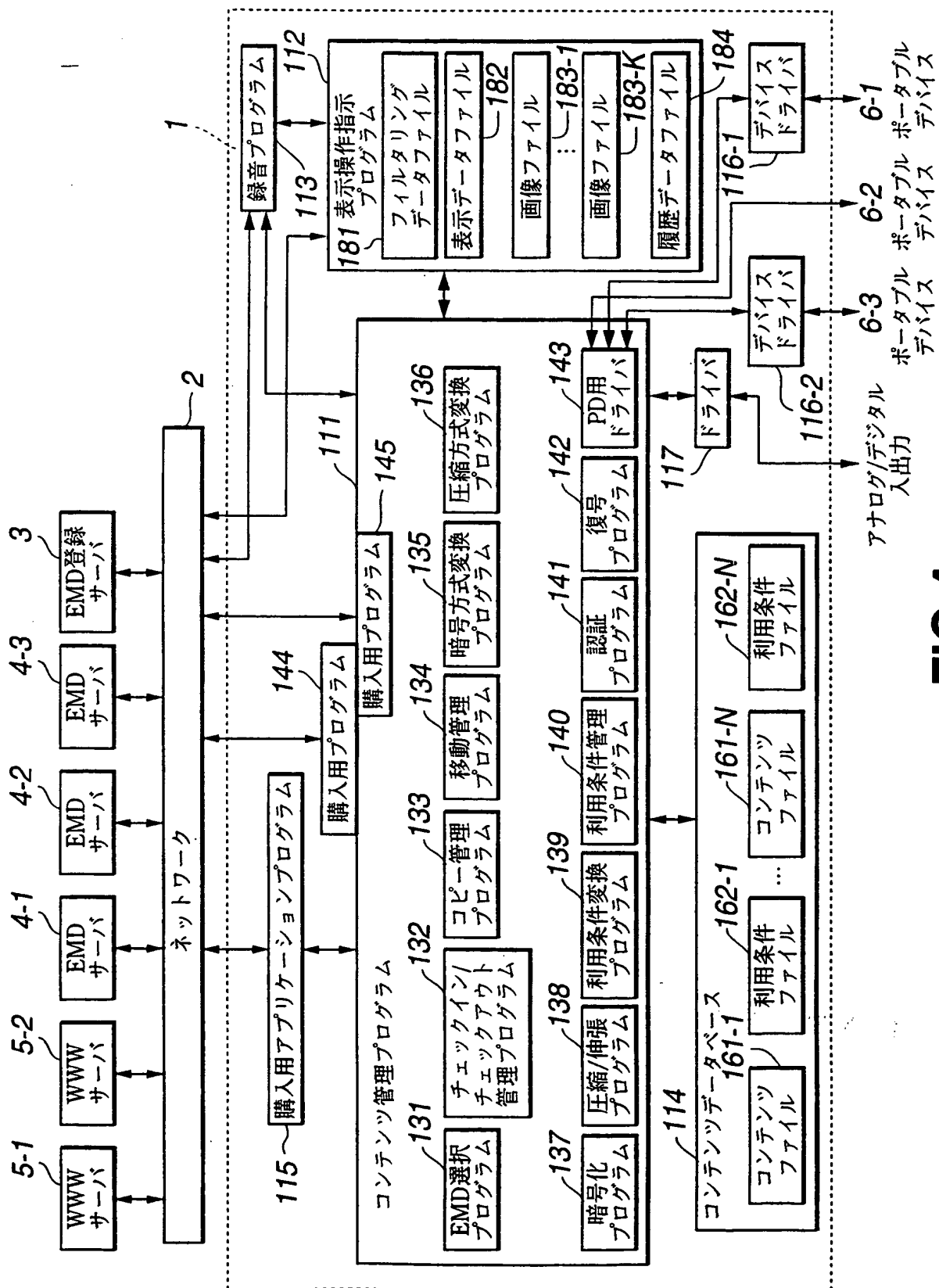


FIG.4

This Page Blank (uspto)

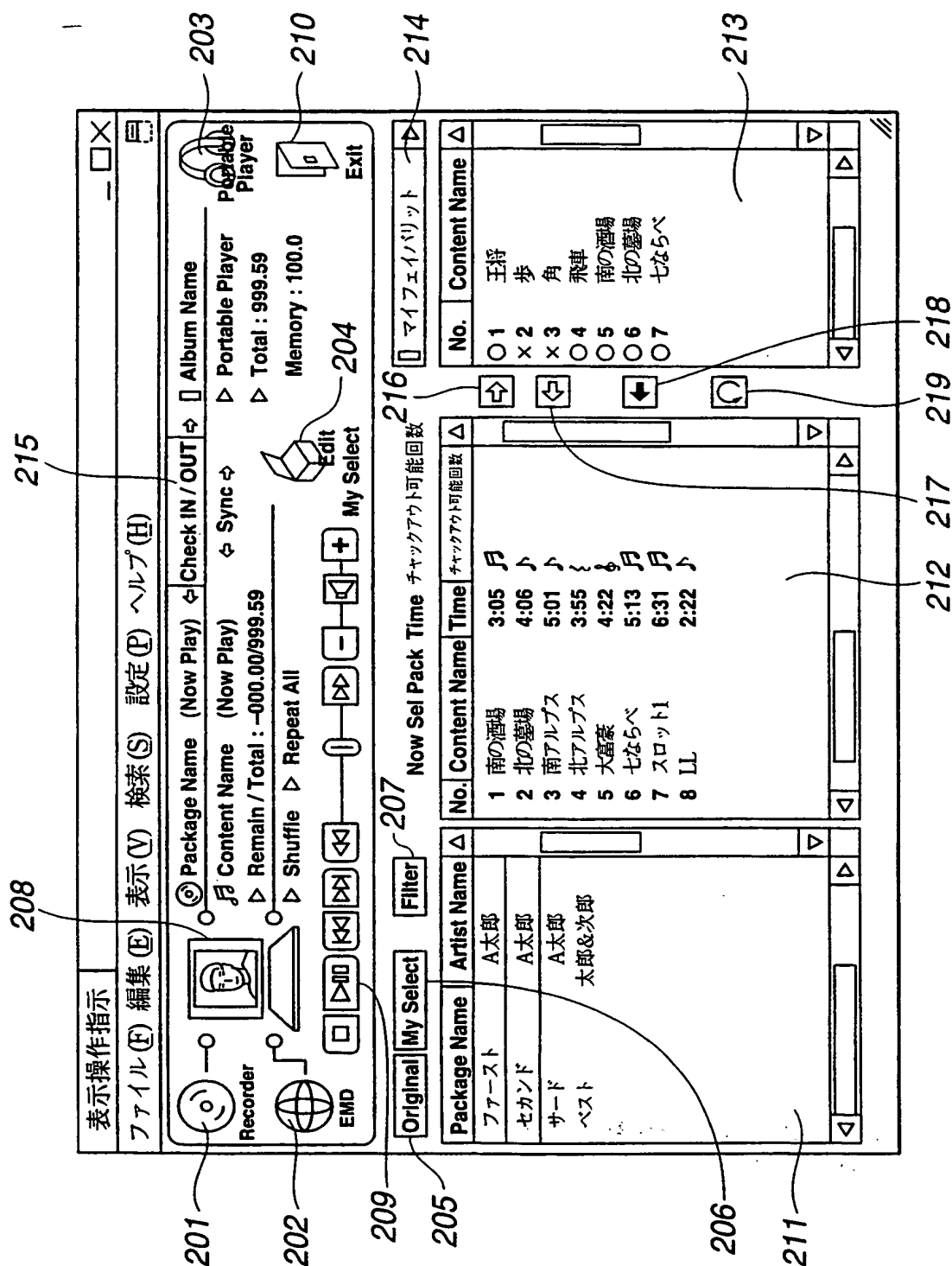


FIG.5

This Page Blank (uspto)

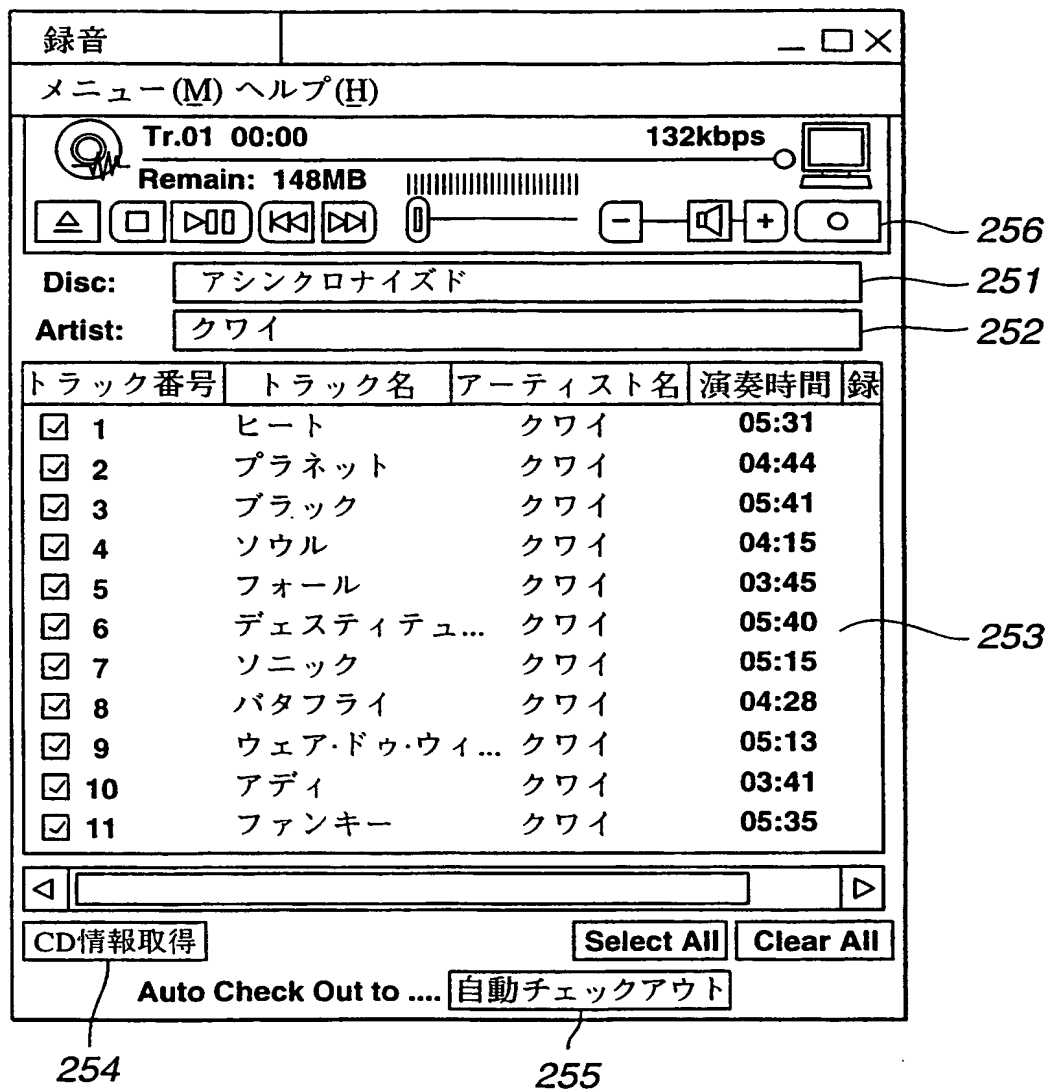


FIG.6

This Page Blank (uspto)

7/36

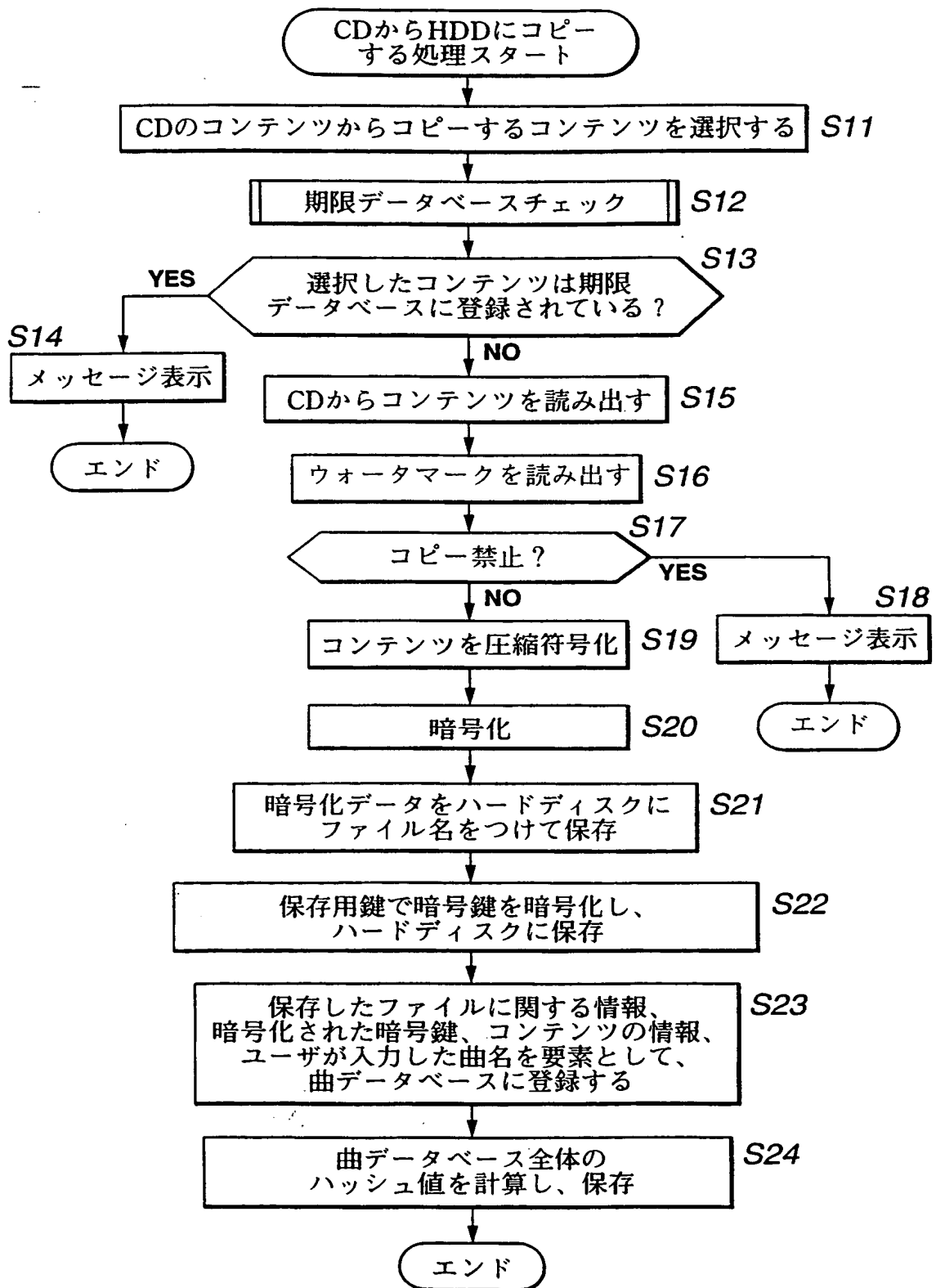


FIG.7

This Page Blank (uspto)

8/36

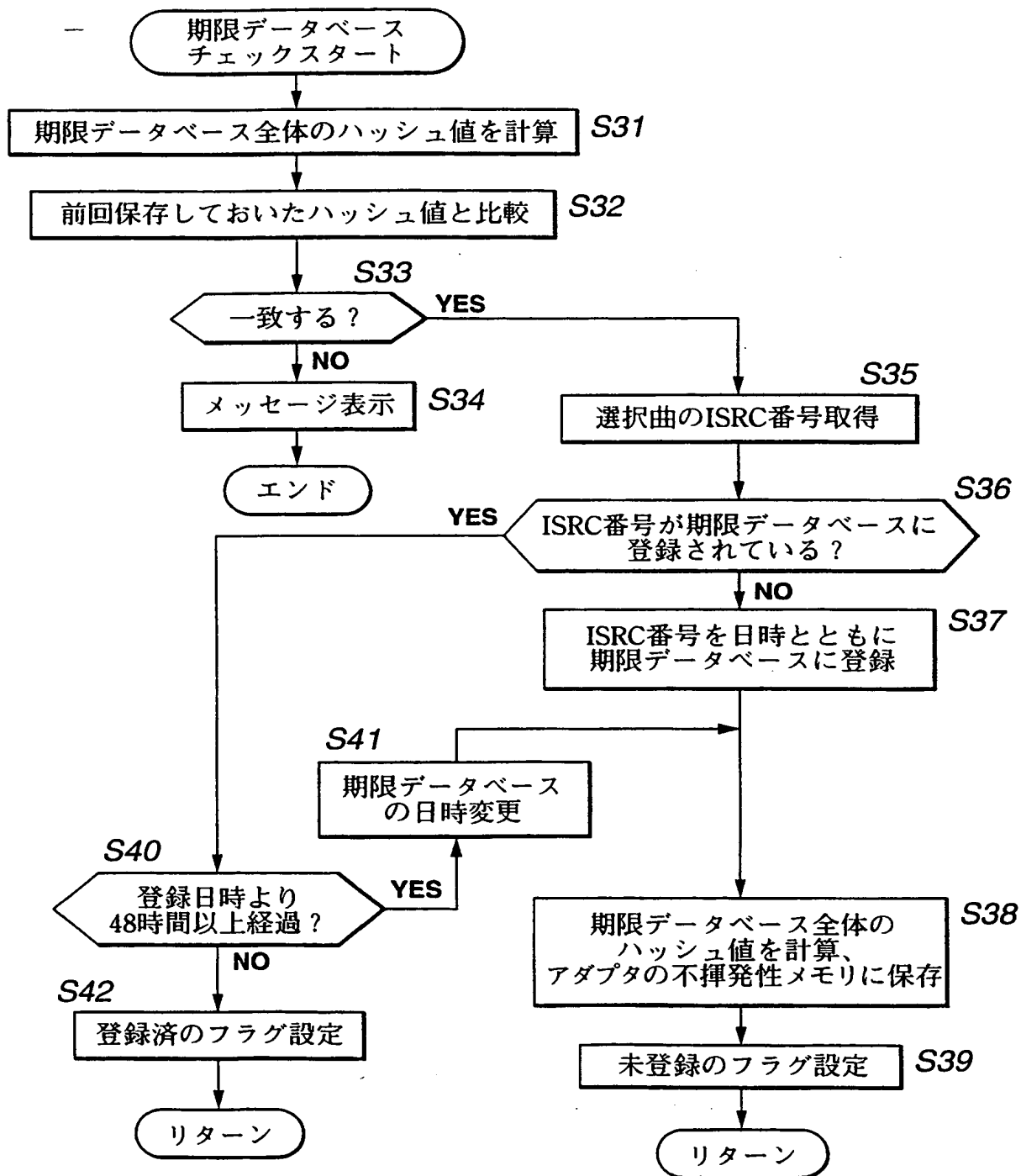


FIG.8

This Page Blank (uspto)

期限データベース

	アイテム 1	アイテム 2	アイテム 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934
-------	----------------

FIG.9

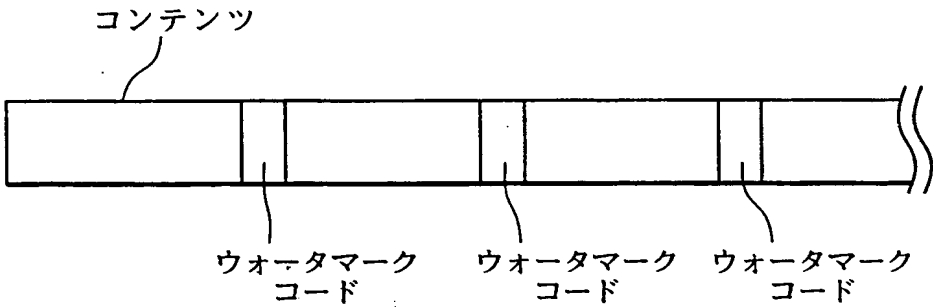


FIG.10

This Page Blank (uspto)

曲データベース

	アイテム 1	アイテム 2	アイテム 3
ファイル名	Xd000110. at2	px92341234. at2	aa0234287034. at2
暗号化された暗号鍵	0xabababababab	0x989898989898989	0x123456789012
曲名	春の小川	運命	荒城の月
長さ	180	190	200
再生条件 : 開始日時	-	2001.01.01.00:00	-
再生条件 : 終了日時	1999.07.31.23:59	-	-
再生条件 : 回数制限	-	20	-
再生回数カウンタ	-	12	-
再生時課金条件	-	-	¥ 5
コピー条件 : 回数	2	0	0
コピー回数カウンタ	1	0	0
コピー条件 : SCMS	0b01	0b10	0b00

ハッシュ値	0xf9951e566321
-------	----------------

FIG.11

This Page Blank (uspto)

11/36

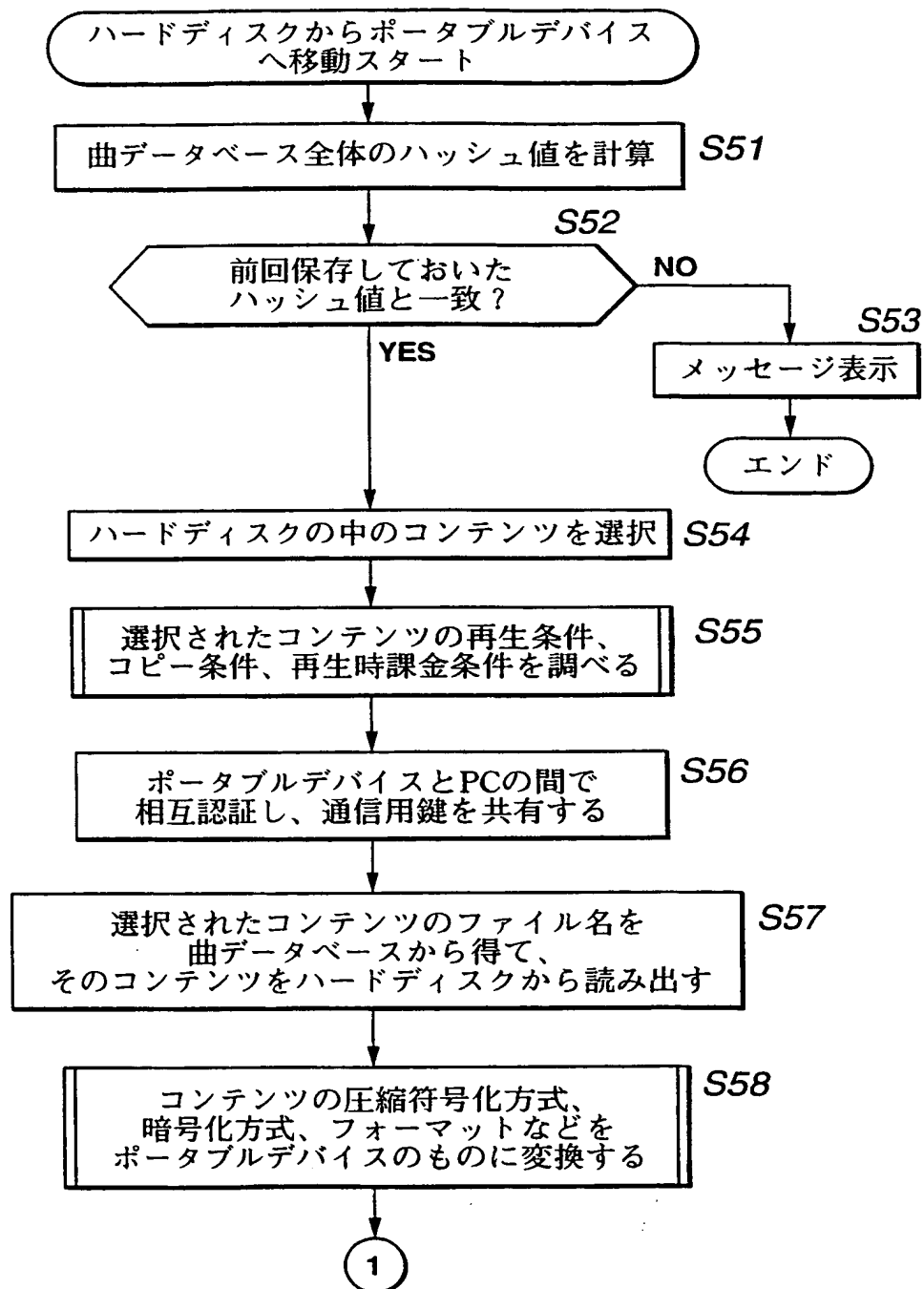


FIG.12

This Page Blank (uspto)

12/36

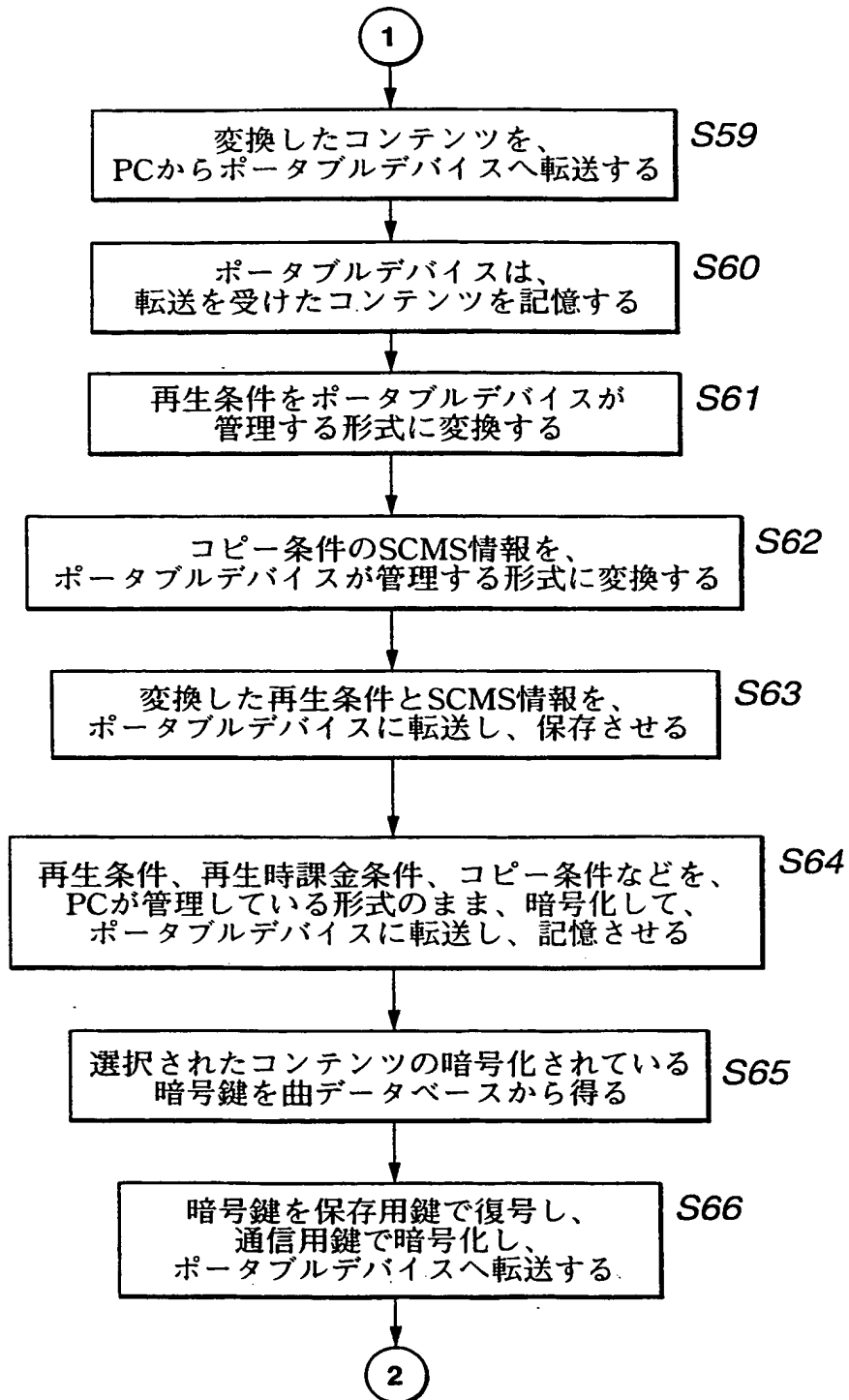


FIG.13

This Page Blank (uspto)

13/36

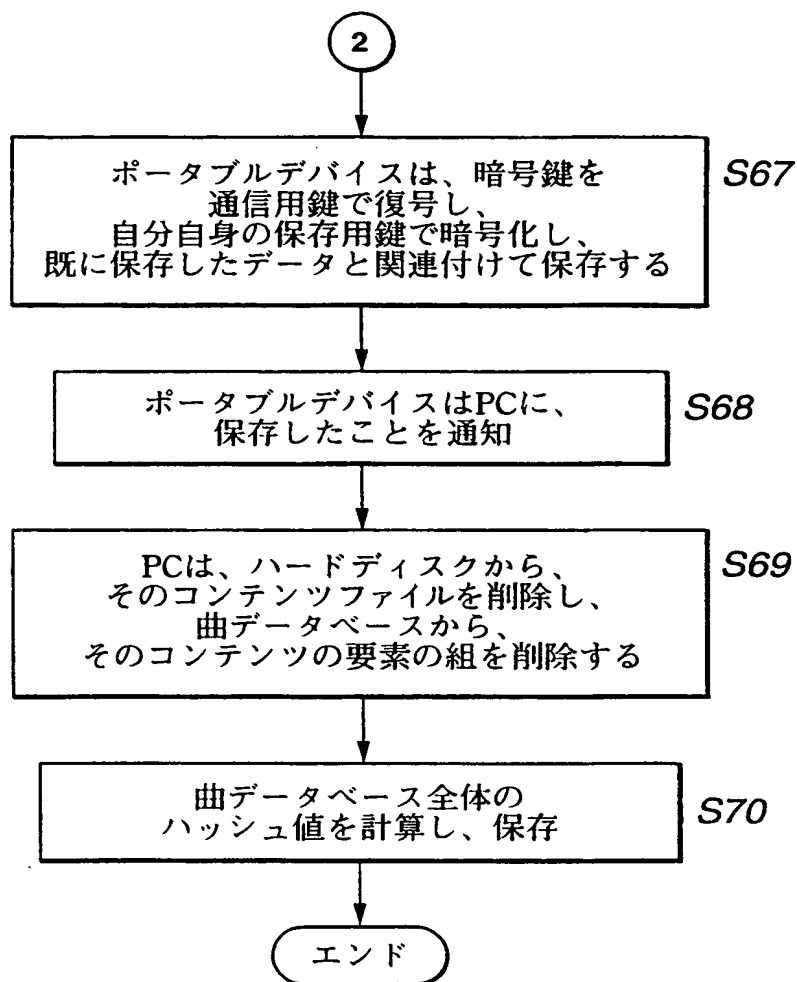


FIG.14

This Page Blank (uspto)

14/36

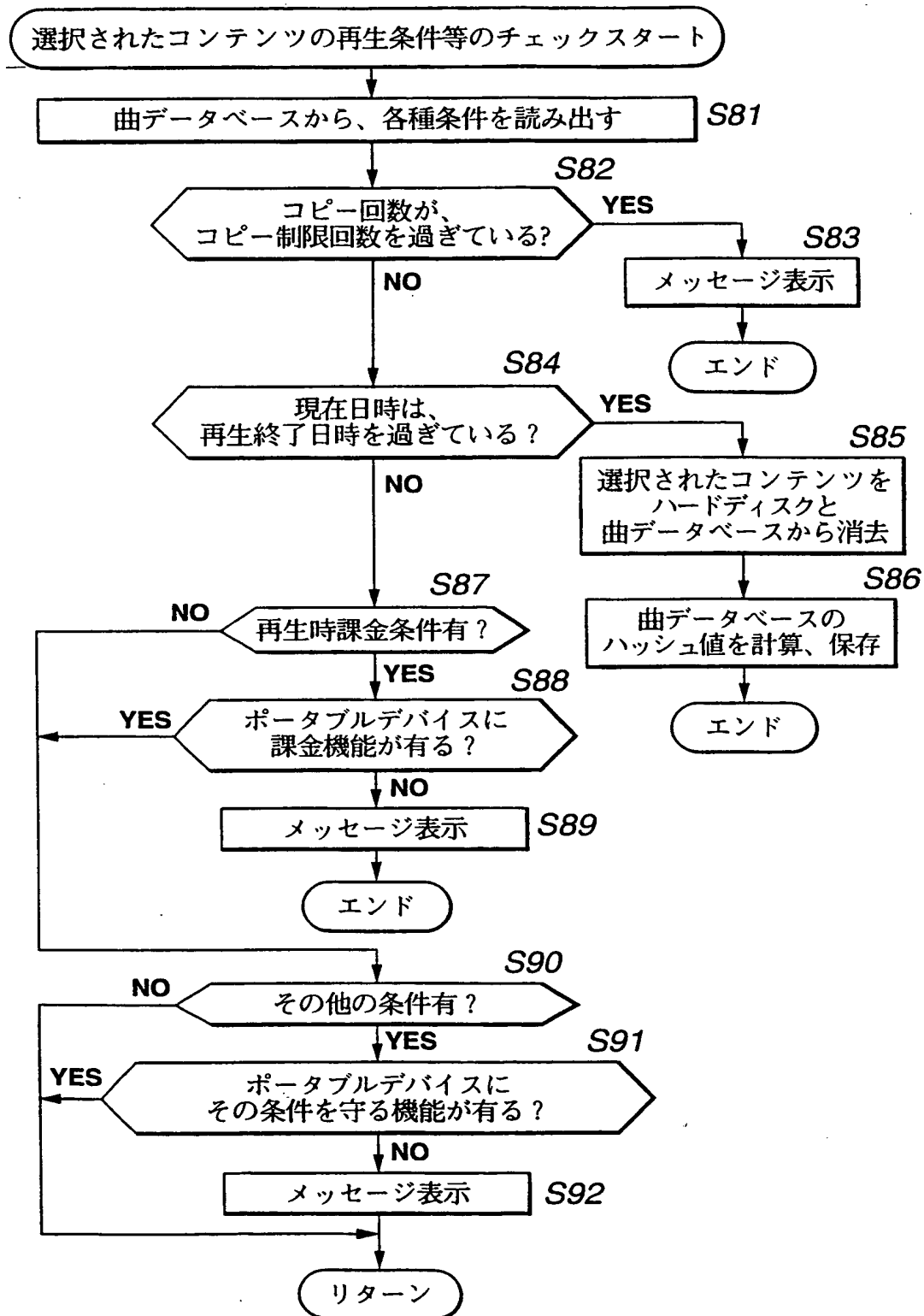


FIG.15

This Page Blank (uspto)

ポータブルデバイスが管理している再生条件

	アイテム 1	アイテム 2	アイテム 3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

FIG.16

This Page Blank (uspto)

16/36

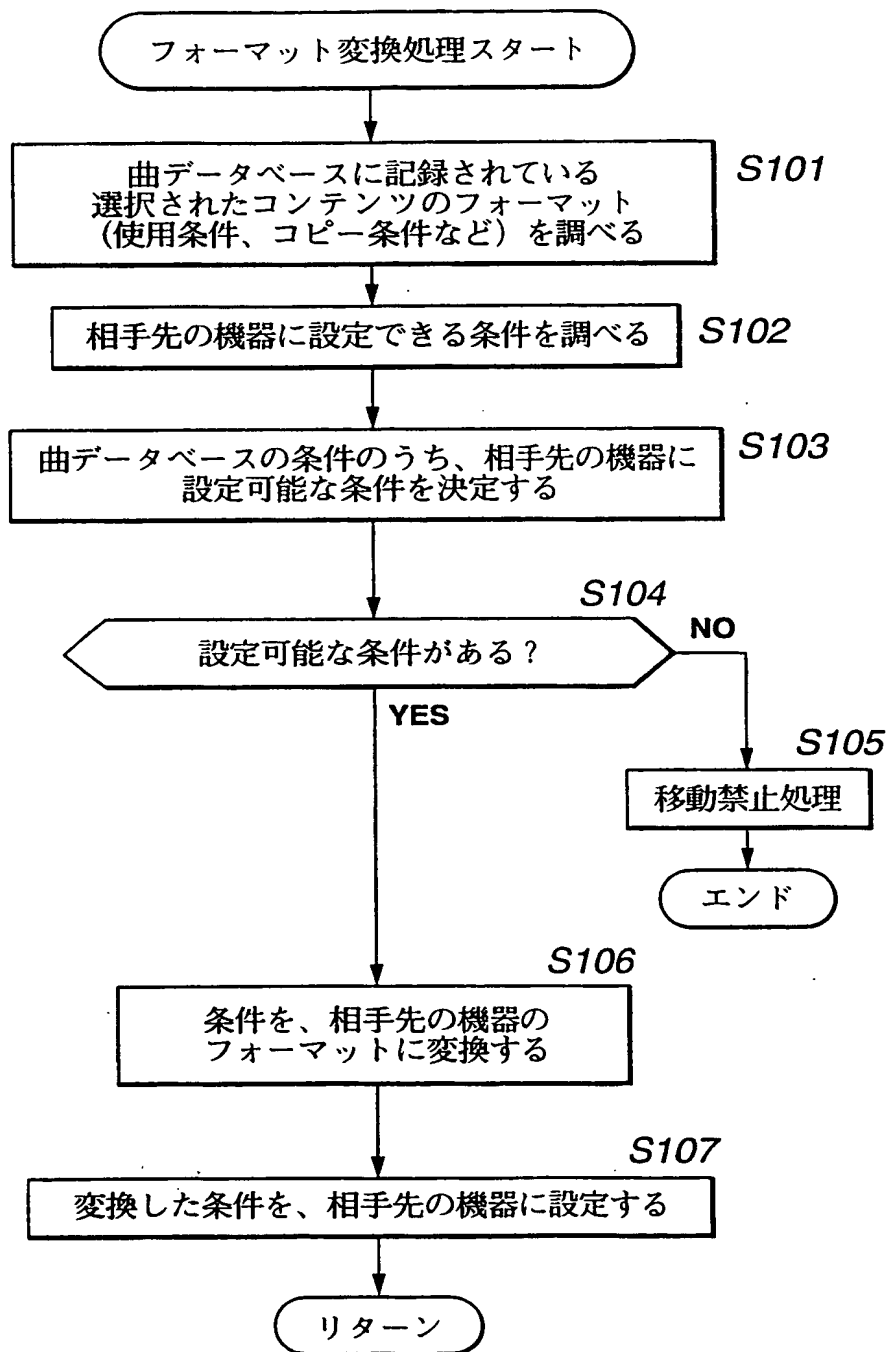


FIG.17

This Page Blank (uspto)

17/36

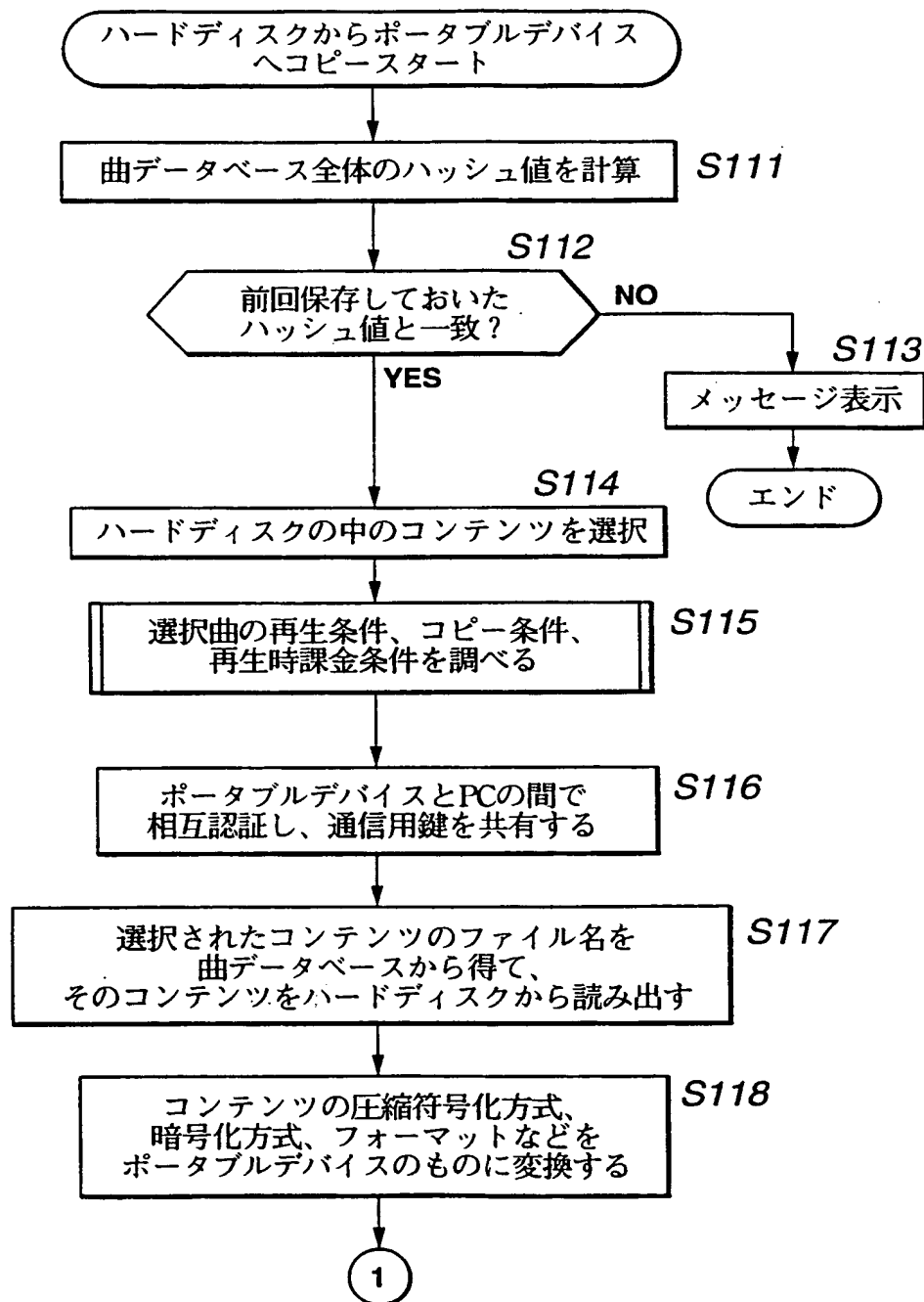


FIG.18

This Page Blank (uspto)

18/36

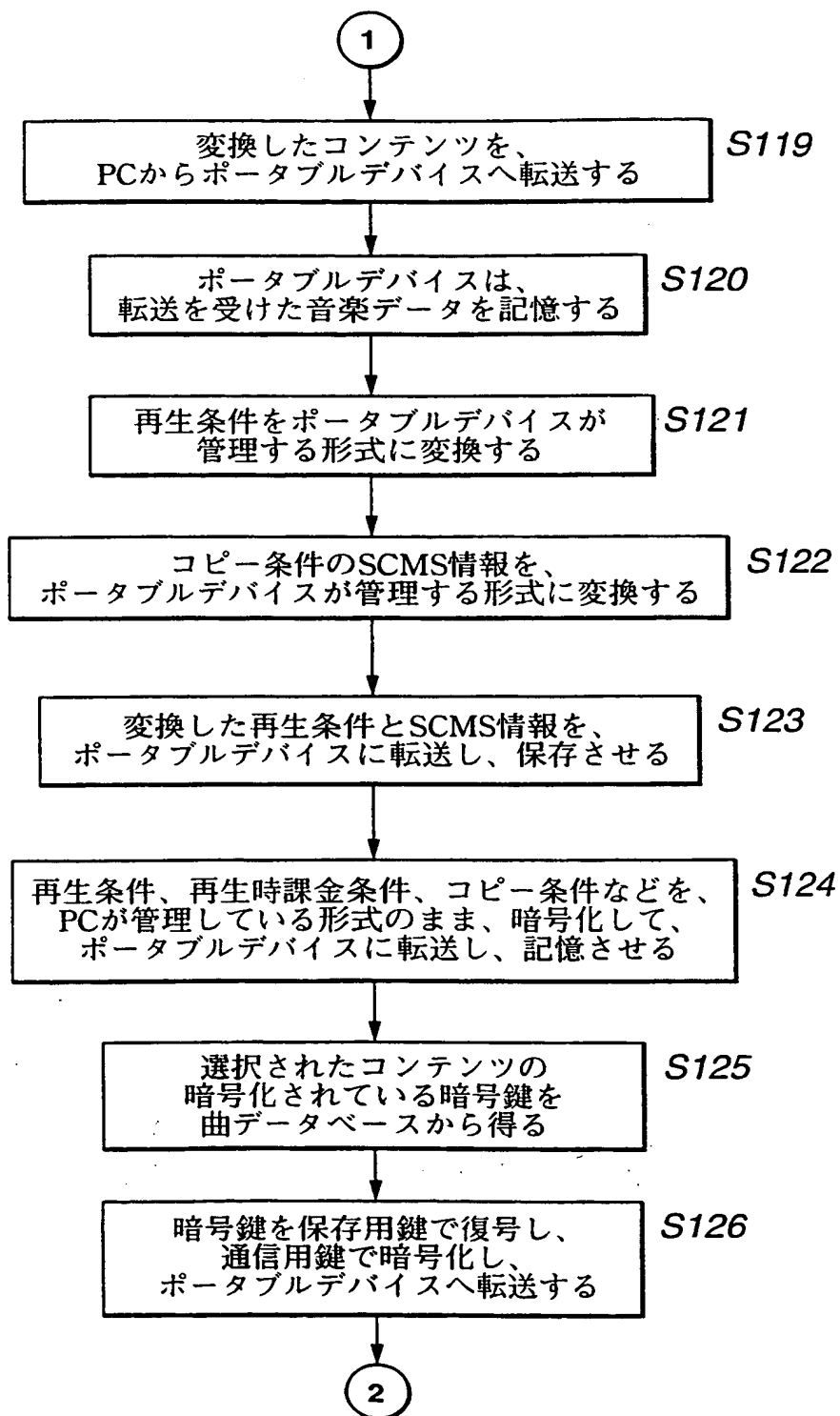


FIG.19

This Page Blank (uspto)

19/36

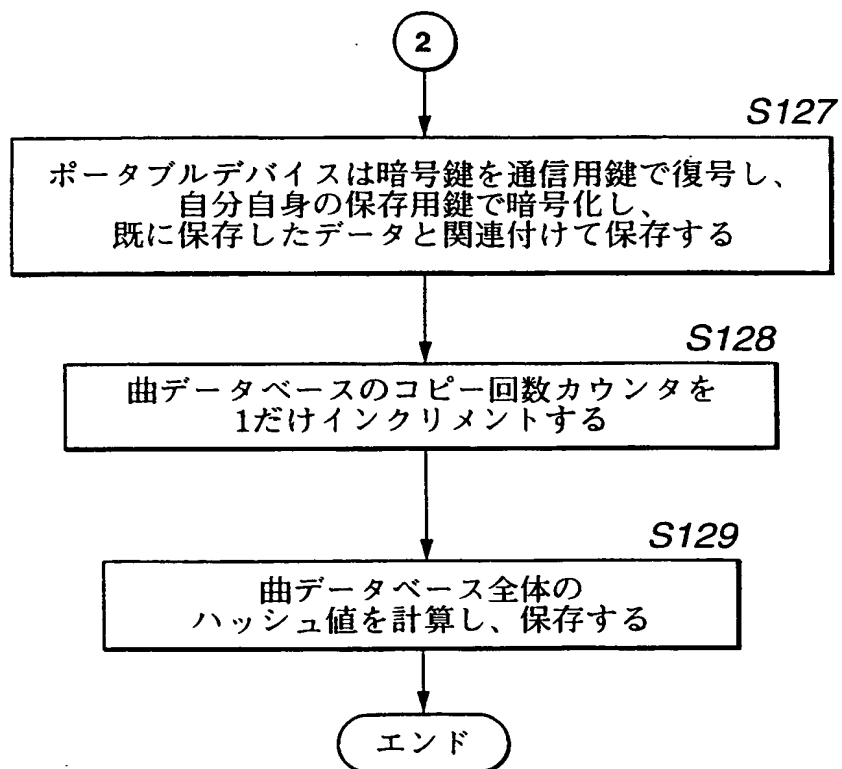


FIG.20

This Page Blank (uspto)

20/36

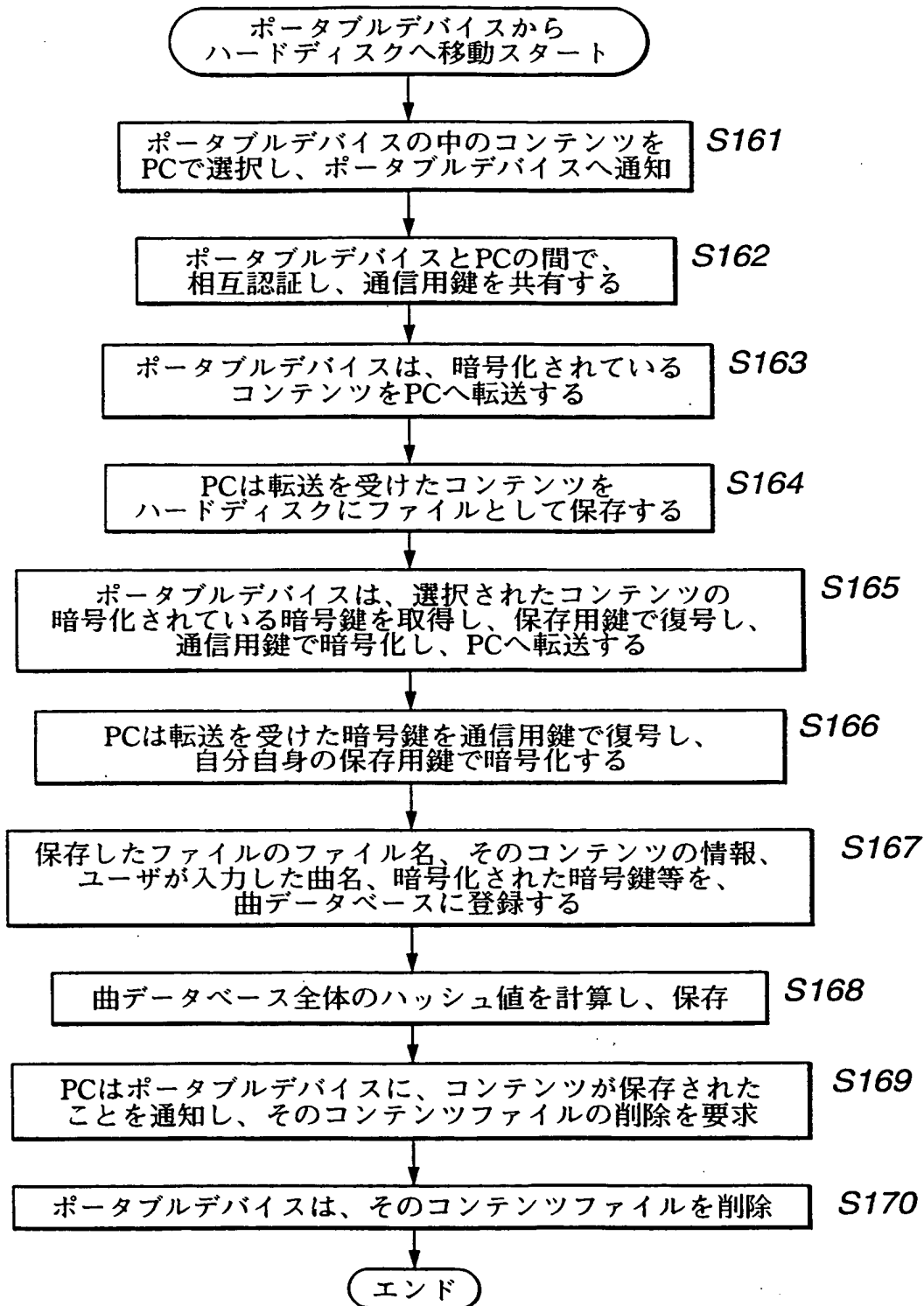


FIG.21

This Page Blank (uspto)

21/36

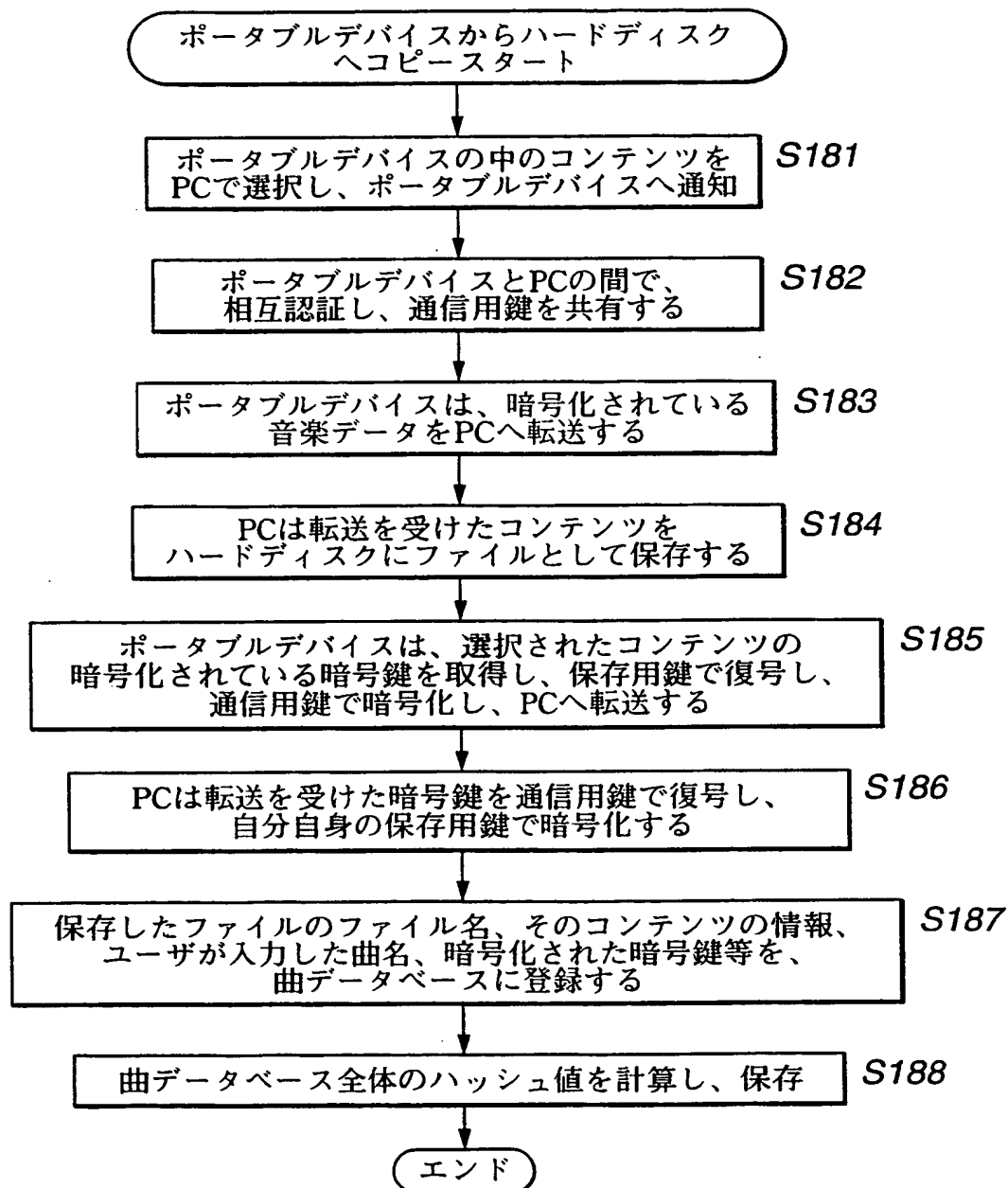


FIG.22

This Page Blank (uspto)

22/36

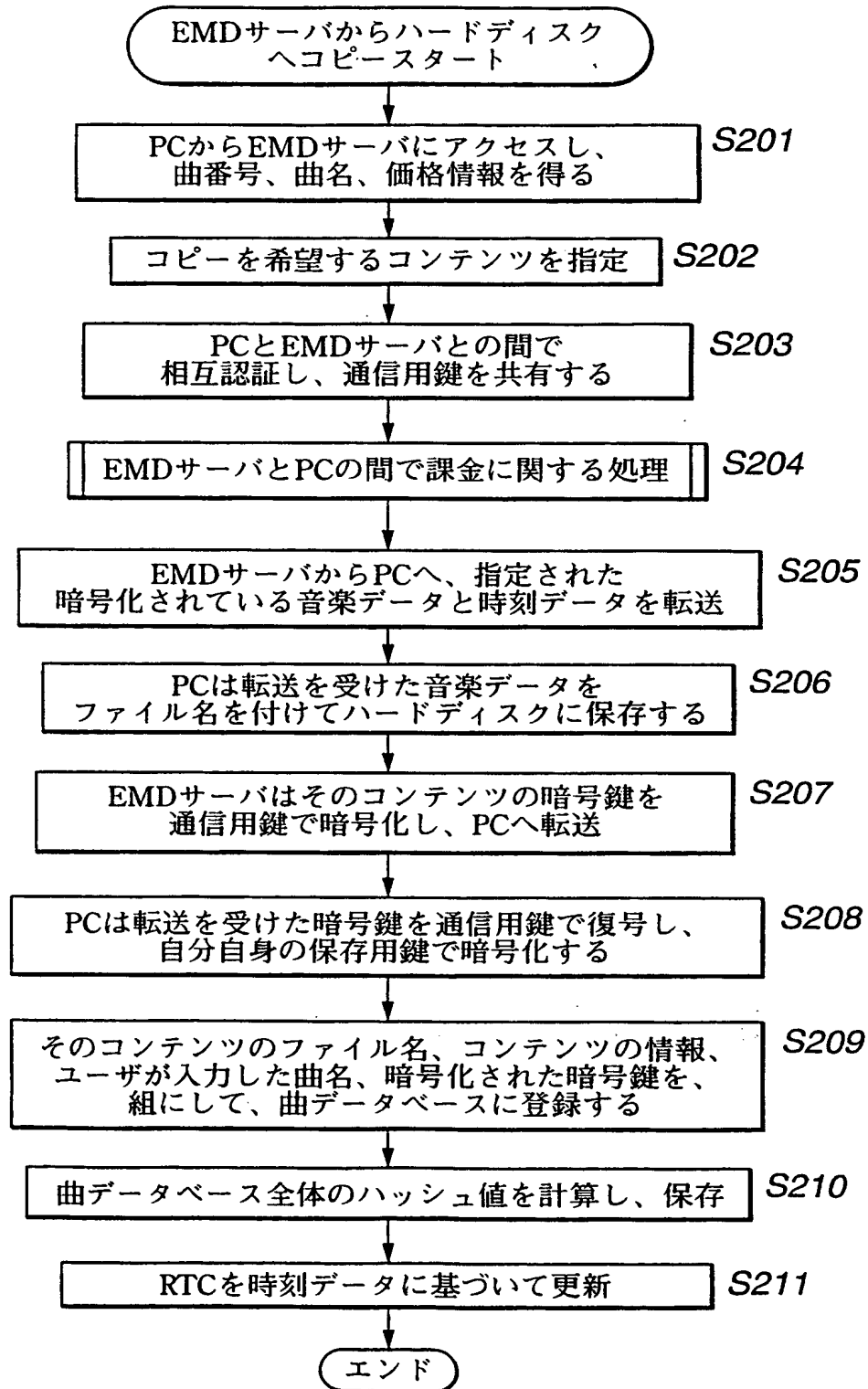


FIG.23

This Page Blank (uspto)

23/36

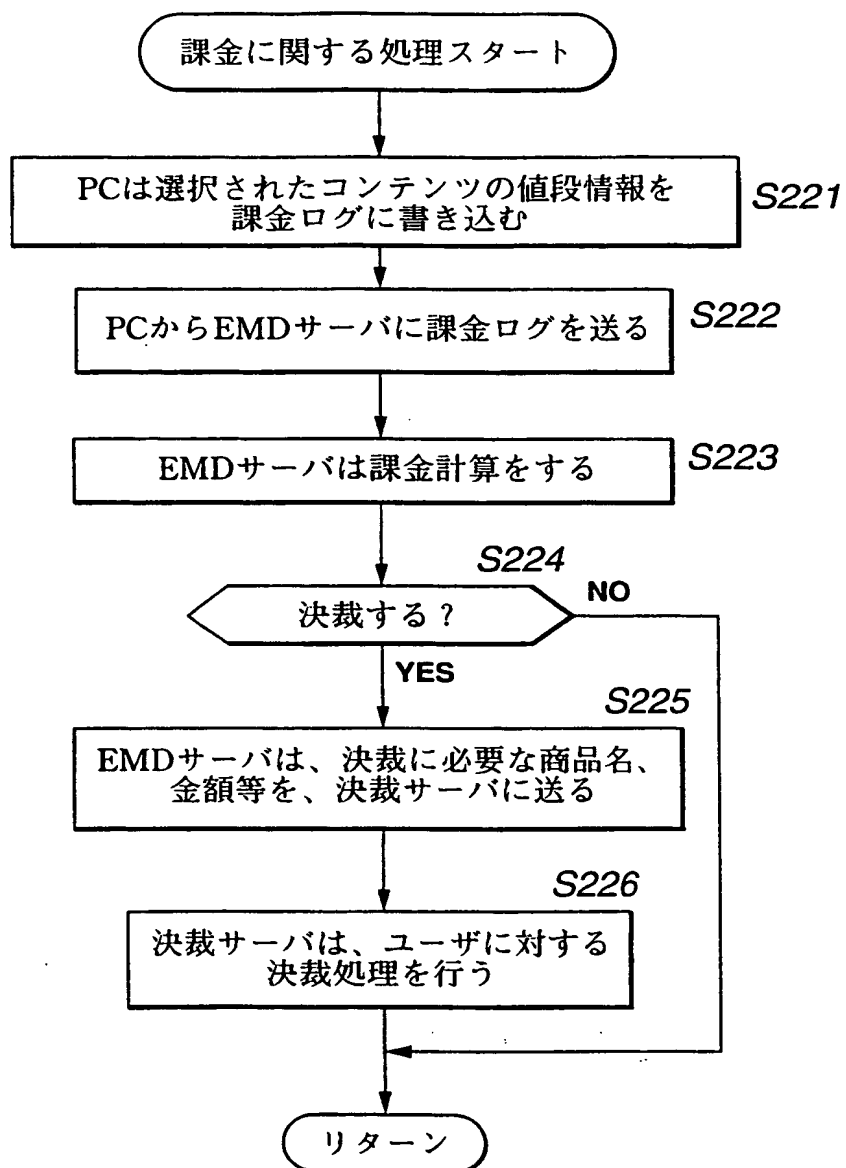


FIG.24

This Page Blank (uspto)

24/36

課金ログ

	アイテム 1	アイテム 2	アイテム 3	
料金	50	50	60	

ハッシュ値	0xf8783e263517
-------	----------------

FIG.25

This Page Blank (uspto)

25/36

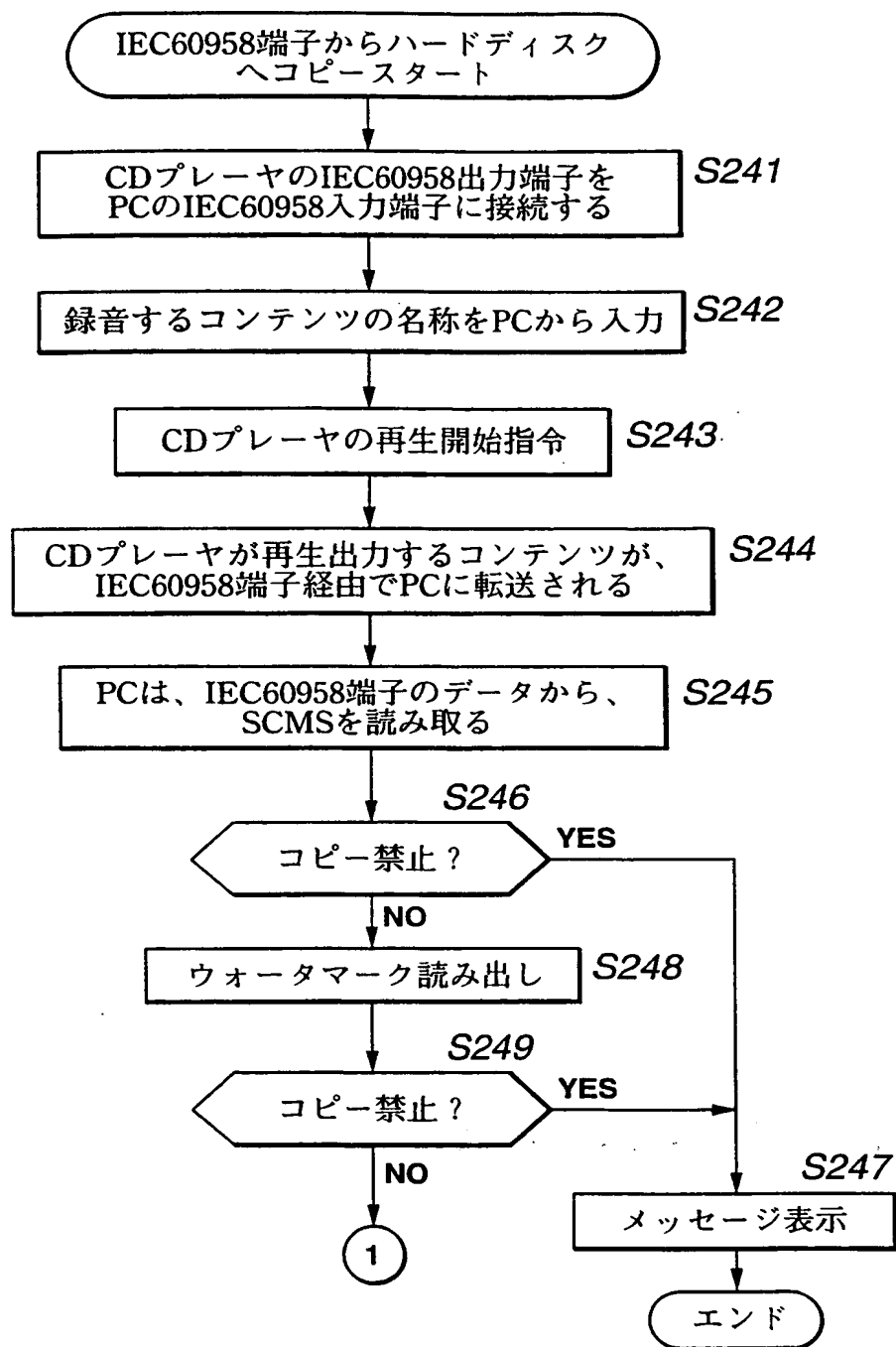


FIG.26

This Page Blank (uspto)

26/36

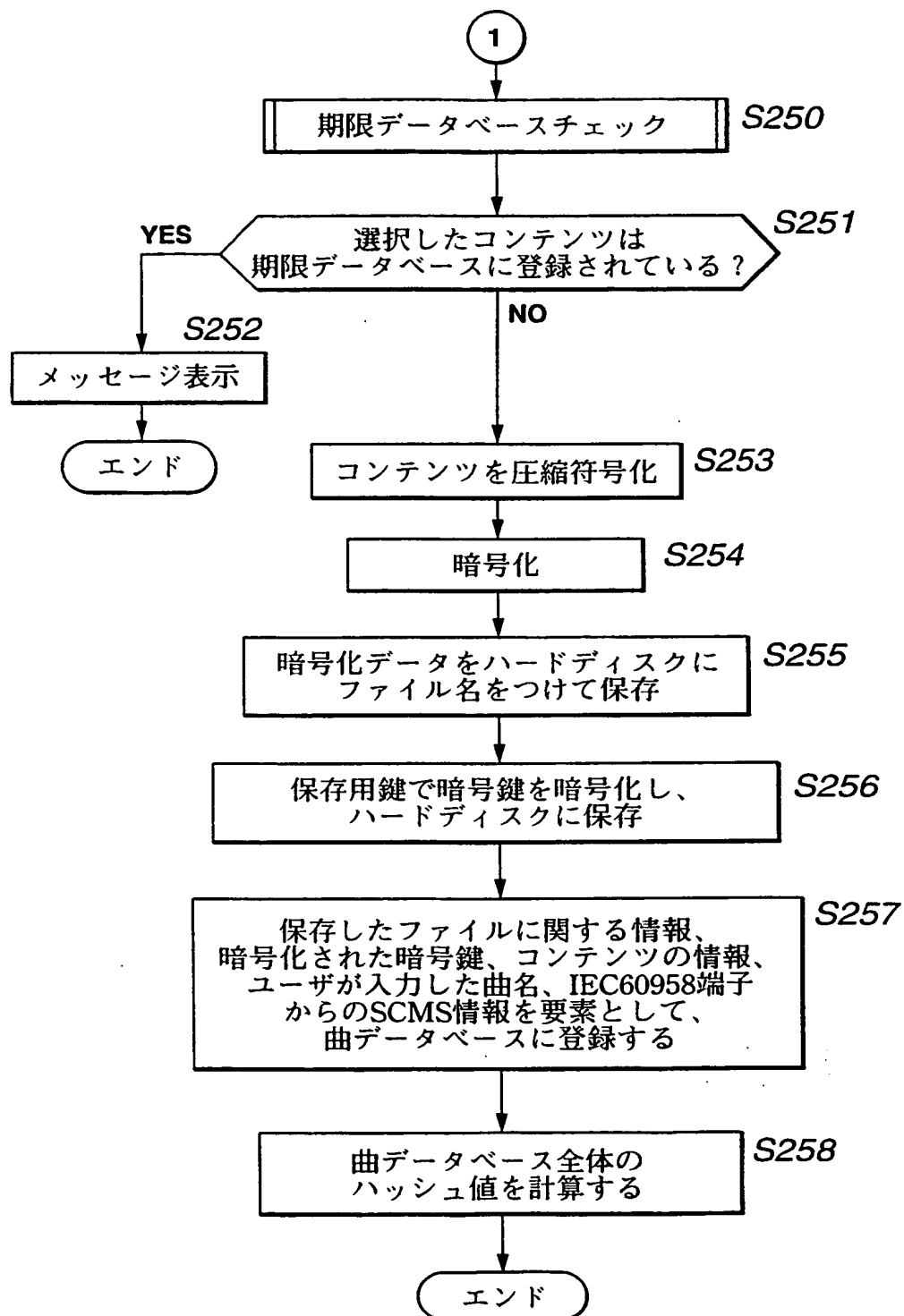


FIG.27

This Page Blank (uspto)

27/36

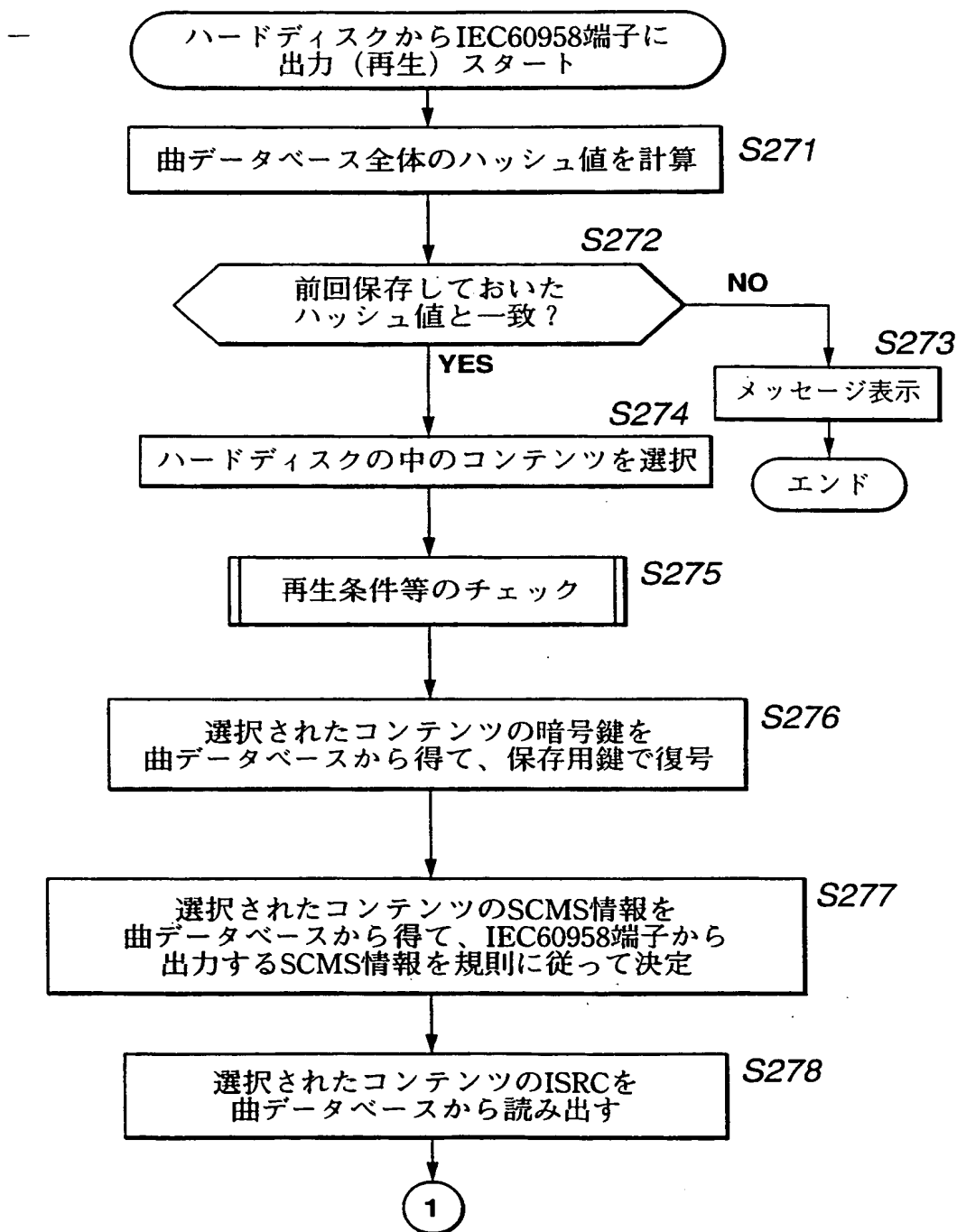


FIG.28

This Page Blank (uspto)

28/36

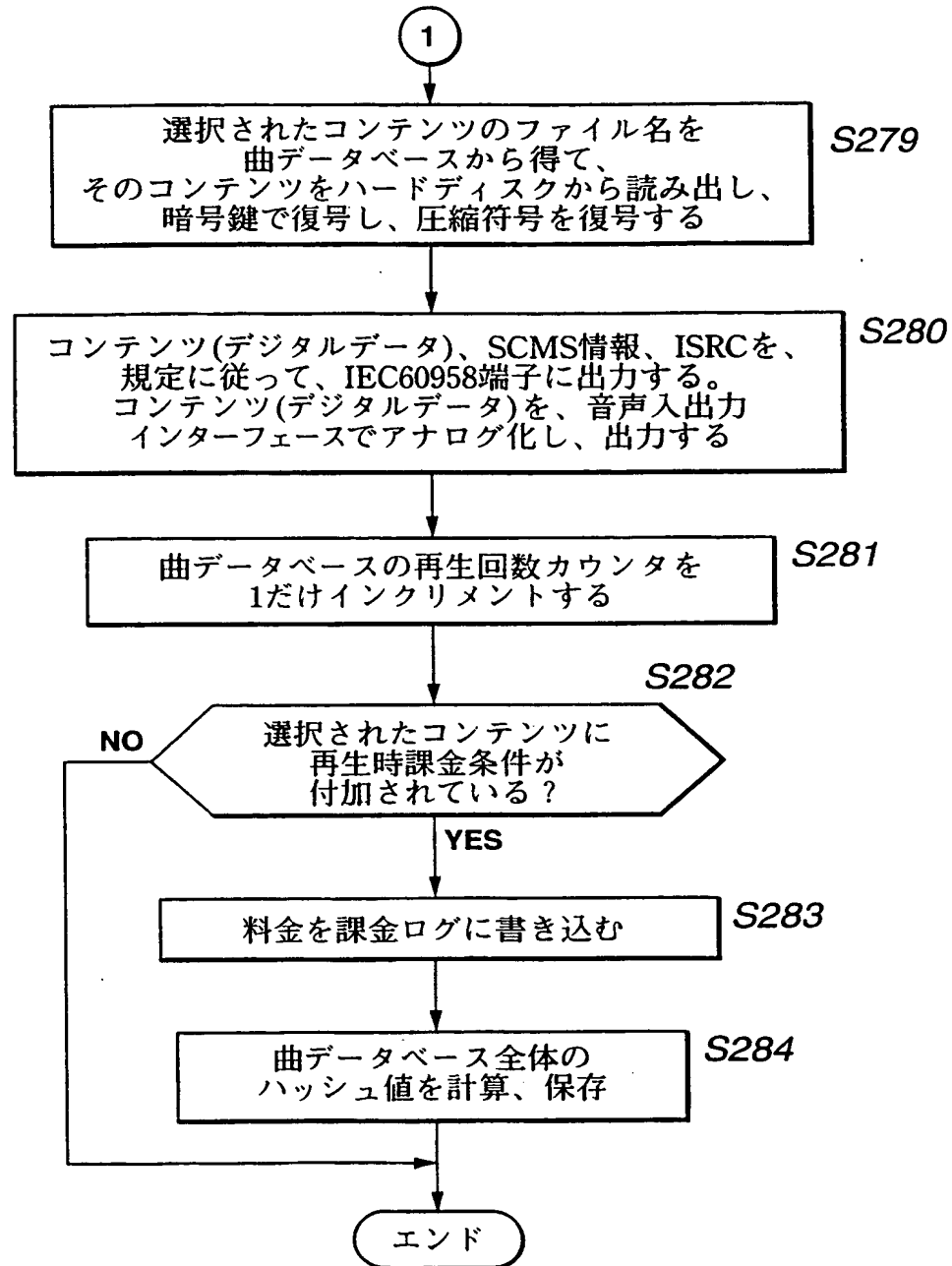


FIG.29

This Page Blank (uspto)

29/36

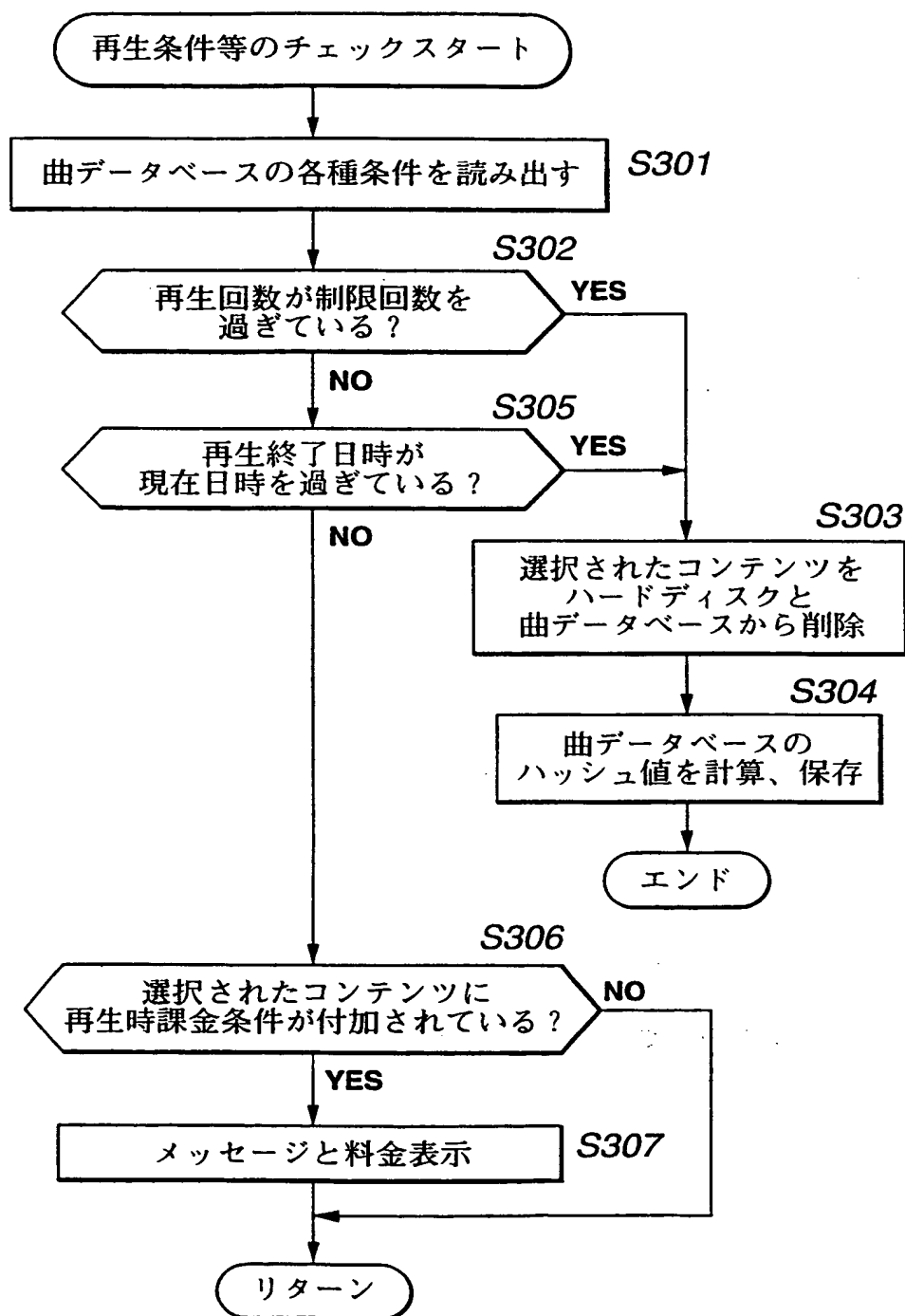


FIG.30

This Page Blank (uspto)

30/36

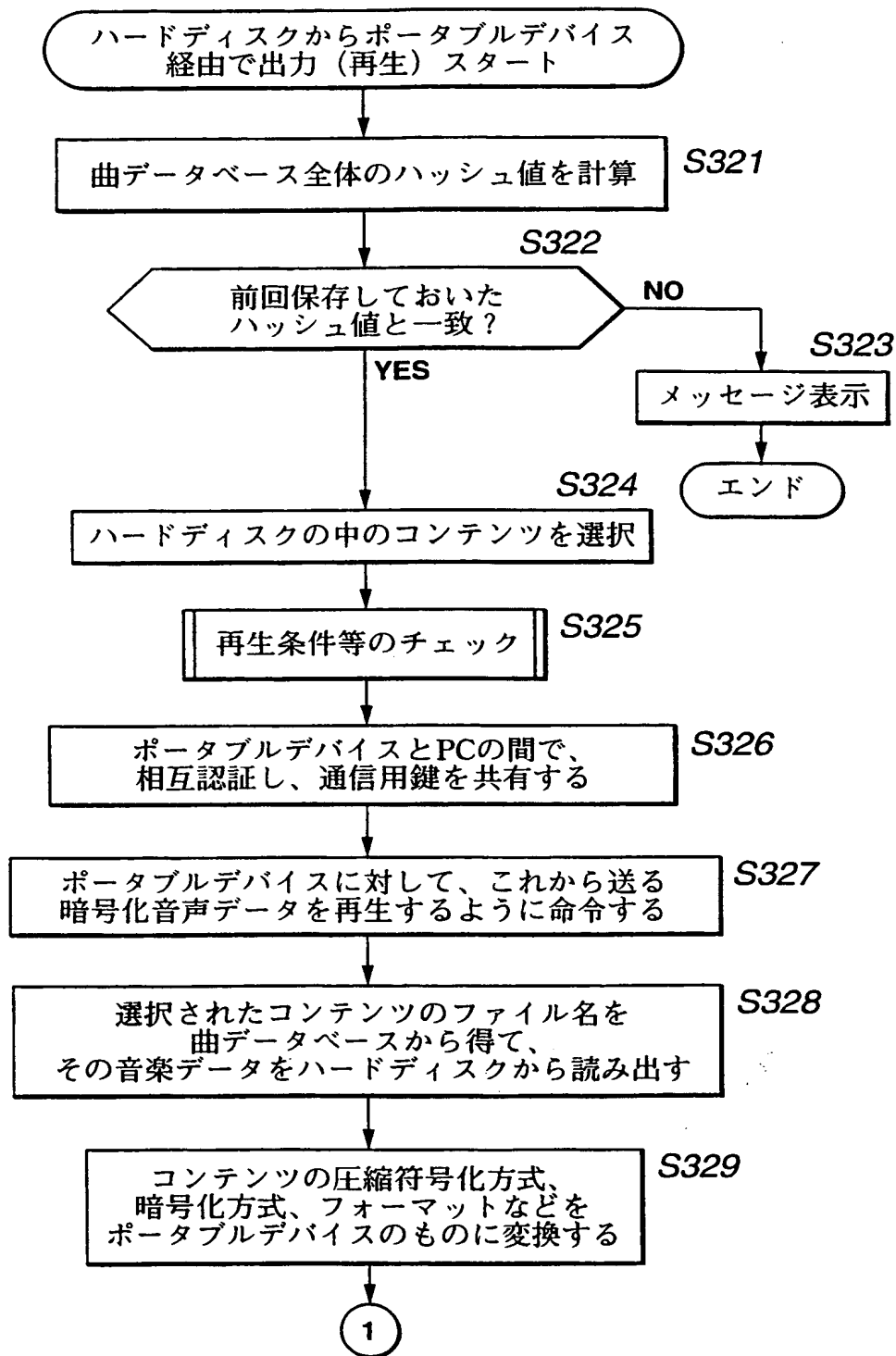


FIG.31

This Page Blank (uspto)

31/36

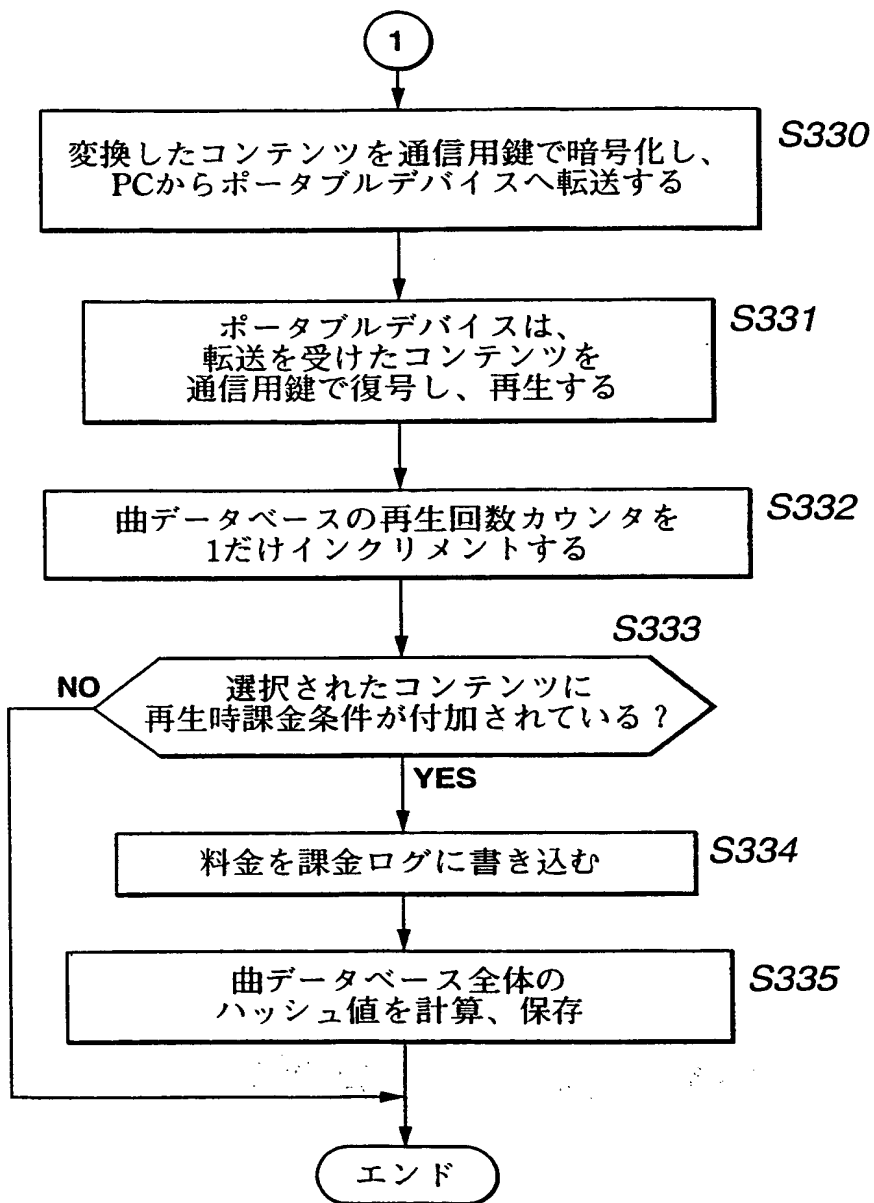


FIG.32

This Page Blank (uspto)

32/36

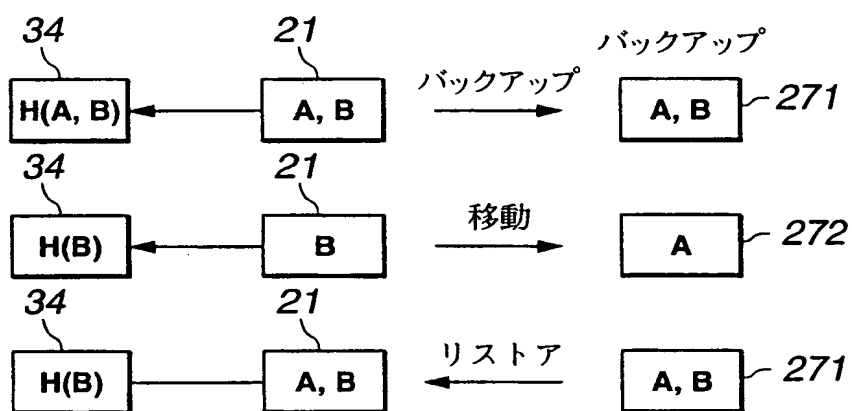


FIG.33

This Page Blank (uspto)

33/36

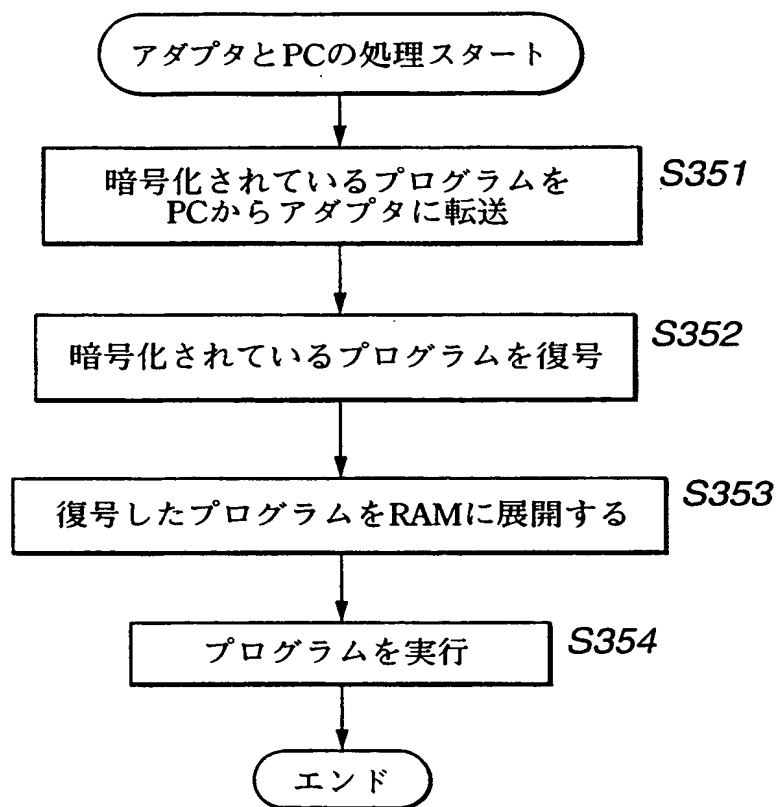


FIG.34

This Page Blank (uspto)

34/36

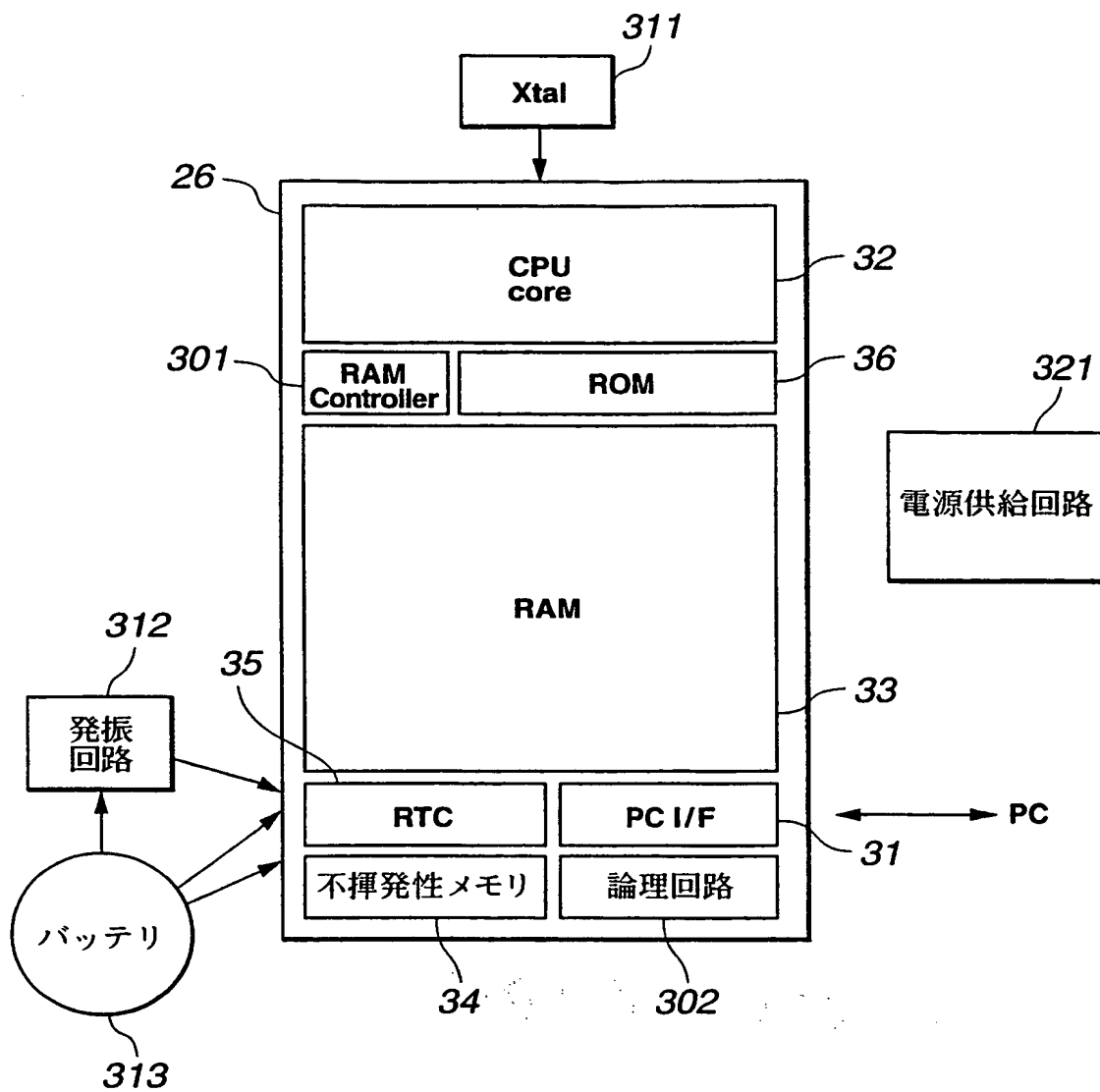
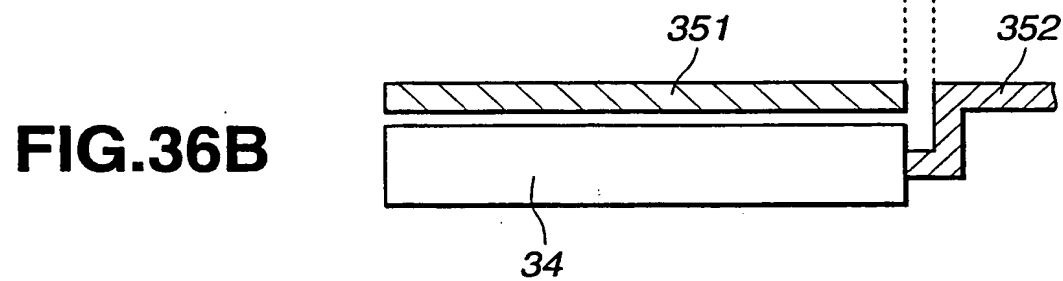
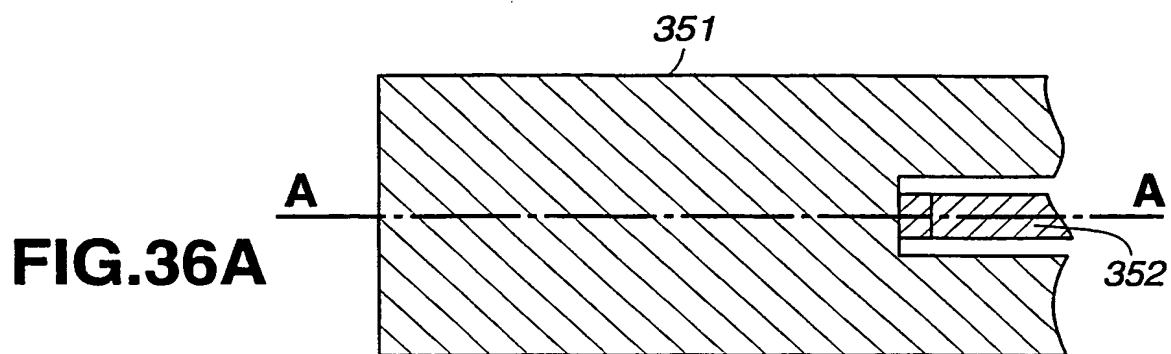


FIG.35

This Page Blank (uspto)

35/36



This Page Blank (uspto)

36/36

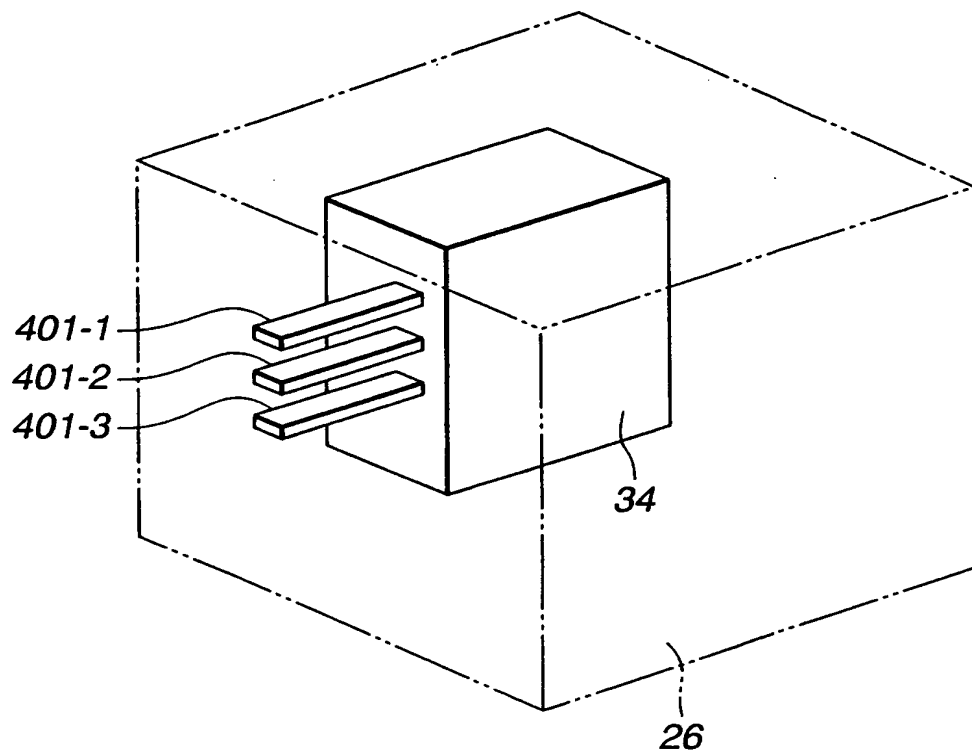


FIG.37

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00904

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl.⁷ G06F15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ G06F15/02, G06F17/60, G06F19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Toroku Jitsuyo Shinan Koho	1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST SCIENCE & TECHNOLOGY DOCUMENT FILE, [CONTENTS*ENCIPHERMENT*ENCODING]

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-283270, A (Fujitsu Limited), 23 October, 1998 (23.10.98), page 9, Column 16, line 29 to page 14, Column 25, line 50 (Family: none)	1-11, 13-23
Y	JP, 10-269289, A (Sony Corporation), 09 October, 1998 (09.10.98), page 5, Column 7, line 3 to page 6, Column 9, line 4 (Family: none)	1-11, 13-23
Y		12
Y	JP, 10-302008, A (Mitsubishi Corporation), 13 November, 1998 (13.11.98), page 9, Column 15, line 33 to page 11, Column 19, line 30 (Family: none)	12

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
16 May, 2000 (16.05.00)Date of mailing of the international search report
30.05.00Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

This Page Blank (uspto)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/02, G06F17/60, G06F19/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2000年
 日本国実用新案登録公報 1996-2000年
 日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICST科学技術文献ファイル, [コンテンツ*暗号化*符号化]

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 10-283270, A (富士通株式会社), 23. 10月. 1998 (23. 10. 98), 第9頁, 第16欄, 第29行-第14頁, 第25欄, 第50行 (ファミリーなし)	1-11, 13-23
Y	JP, 10-269289, A (ソニー株式会社), 9. 10月. 1998 (09. 10. 98), 第5頁, 第7欄, 第3行-第6	1-11, 13-23
Y	頁, 第9欄, 第4行 (ファミリーなし)	12
Y	JP, 10-302008, A (三菱商事株式会社), 13. 11月. 1998 (13. 11. 98), 第9頁, 第15欄, 第33行-第11頁, 第19欄, 第30行 (ファミリーなし)	12

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

16. 05. 00

国際調査報告の発送日

30.05.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

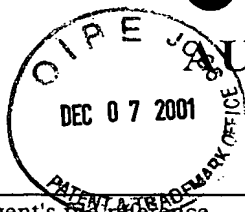
石井 茂和

5M

8837

電話番号 03-3581-1101 内線 6438

This Page Blank (uspto)



AUSTRALIAN PATENT OFFICE SEARCH REPORT

RECEIVED
DEC 11 2001
Technology Center 2100

Applicant's or agent's full name 688SG67/GM/LYW/IR		
Application No. SG 0005721-6	Application Filing Date (day/month/year) 17 February 2000	(Earliest) Priority Date (day/month/year) 17 February 1999
Applicant Sony Corporation		

This search report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. ☐ Certain claims were found unsearchable (See Box I)
2. ☐ Unity of invention is lacking (See Box II)
3. ☐ The application contains disclosure of a nucleotide and/or amino acid sequence listing and the search was carried out on the basis of the sequence listing
 - ☐ filed with the application
 - ☐ furnished by the applicant separately from the application,
 - ☐ but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in application as filed
4. With regard to the title
 - ☒ the text is approved as submitted by the applicant.
 - ☐ the text has been established by this Office to read as follows:
5. With regard to the abstract,
 - ☒ the text is approved as submitted by the applicant
 - ☐ the text has been established by this Office as it appears in Box III
6. The figure of the drawings to be published with the abstract is:
Figure No. 2
 - ☒ as suggested by the applicant.
 - ☐ because the applicant failed to suggest a figure
 - ☐ because this figure better characterises the invention
 - ☐ None of the figures

RECEIVED
IPOS
SEP 20 16:14

This Page Blank (uspto)

**AUSTRALIAN PATENT OFFICE
SEARCH REPORT**

Application No.
SG 0005721-6

A. CLASSIFICATION OF SUBJECT MATTER

According to International Patent Classification (IPC)

Int. Cl. ⁷ G06F 15/02, 12/14, 9/06

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the search (name of data base and, where practicable, search terms used)

WPAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Patent Abstract of Japan, JP10269289 (Sony Corp) 09 October 1998 (supplied from the esp@cenet database)	
A	Patent Abstract of Japan, JP10283270 (Fujitsu Ltd) 23 October 1998(supplied from the esp@cenet database)	
A	EP0878753A2 (Mitsubishi Corporation) 18 November 1998	

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

*Special categories of cited documents:		"T"	Later document published after the filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document but published on or after the filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the filing date but later than the priority date claimed		

Date of submission of the request to the Australian Patent Office 9 July 2001	Date of completion of the search report 12 September 2001	Date of mailing of the search report 19 September 2001
--	--	---

Name and mailing address AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. 61 2 62853929	Authorised officer M. EMAMI
---	------------------------------------

This Page Blank (uspio)

**AUSTRALIAN PATENT OFFICE
SEARCH REPORT**

**PATENT FAMILY
MEMBERS**

Application No.
SG 0005721-6

Patent Document Cited in Search Report		Patent Family Member	
EP	878753	JP	10302008
JP	10269289	NONE	
JP	10283270	NONE	
END OF ANNEX			

This Page Blank (uspto)

AUSTRALIAN PATENT OFFICE

EXAMINATION REPORT

Applicant's or agents file reference 688SG67/GM/LYW/IR		
Application No. SG 0005721-6	Application Filing Date (<i>day/month/year</i>) 17 February 2000	Priority Date (<i>day/month/year</i>) 17 February 1999
International Patent Classification (IPC) as indicated in the search report or the Request, if no indication in the search report Int. Cl. ⁷ G06F 15/02, 12/14, 9/06		
Applicant Sony Corporation		

1.	This REPORT consists of a total of 4 sheets.
2.	<p>This report contains indications relating to the following items:</p> <div style="margin-left: 20px;"> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>III <input type="checkbox"/> Lack of unity of invention</p> <p>IV <input checked="" type="checkbox"/> Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>V <input type="checkbox"/> Certain documents cited</p> <p>VI <input type="checkbox"/> Certain defects in the application</p> <p>VII <input checked="" type="checkbox"/> Certain observations on the application</p> </div>
3.	This report is based upon the assumption that the priority claim is valid.
4.	The search report used was issued by the Australian Patent Office and the date of completion is 12 September 2001.

01 SEP 20 16:14

IPOS
RECEIVED

Date of submission of the request to the Australian Patent Office 9 July 2001	Date of mailing of the report <i>19 September 2001</i>
Name and mailing address AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. 61 2 62853929	Authorized Officer M. EMAMI

This Page Blank (uspto)

AUSTRALIAN PATENT OFFICE
EXAMINATION REPORT

Application No.

SG 0005721-6

I. Basis of the report

1. This report has been drawn on the basis of

☒ the application as originally filed.

☐ the description, pages , as originally filed,
 pages , filed with the request,
 pages , received on with the letter of
 pages , received on with the letter of

☐ the claims, pages , as originally filed,
 pages , filed with the request,
 pages , received on with the letter of
 pages , received on with the letter of

☐ the drawings, sheets/fig. , as originally filed,
 sheets/fig. , filed with the request,
 sheets/fig. , received on with the letter of

2. The amendments have resulted in the cancellation of: pages:

 sheets of drawings/figures No:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box

4. Additional observations, if necessary:

This Page Blank (uspto)

AUSTRALIAN PATENT OFFICE
EXAMINATION REPORT

Application No.
SG 0005721-6

IV. Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims 1-35	YES
	Claims	NO
Inventive step (IS)	Claims 1-35	YES
	Claims	NO
Industrial applicability (IA)	Claims 1-35	YES
	Claims	NO

2. CITATIONS AND EXPLANATIONS

JP 10269289
JP 10283270
EP 0878753

The above documents, from the search report, are the most relevant prior art to the invention. The essential feature of the invention that is "controlling storage or read of the data compressed at the compressing step and encrypted at the encrypting step" or "controlling storage or read of content data into or from the content data storage means based on the result of the program execution by a program executing means" is not disclosed in the above documents. Therefore, the invention defined in any of the claims 1-35 is novel and inventive.

This Page Blank (uspto)

AUSTRALIAN PATENT OFFICE
EXAMINATION REPORT

Application No.

SG 0005721-6

VII. Certain observations on the application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

☒ The claimed invention is patentable according to Section 13(3); or

☐ The claimed invention is unpatentable according to Section 13(3) because:

This Page Blank (uspto)

PCT

E P



国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 SK00PCT17	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JP00/00904	国際出願日 (日.月.年) 17.02.00	優先日 (日.月.年) 17.02.99
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

- a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。
- b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。
☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
 第 2 図とする。 ☒ 出願人が示したとおりである。 ☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)

A. 発明の属する分野の分類 (国際特許分類 (IPC)).

Int. Cl⁷ G06F15/02

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/02, G06F17/60, G06F19/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2000年
 日本国実用新案登録公報 1996-2000年
 日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICST 科学技術文献ファイル, [コンテンツ*暗号化*符号化]

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 10-283270, A (富士通株式会社), 23. 10 月. 1998 (23. 10. 98), 第9頁, 第16欄, 第29行 -第14頁, 第25欄, 第50行 (ファミリーなし)	1-11, 13-23
Y	J P, 10-269289, A (ソニー株式会社), 9. 10月. 1998 (09. 10. 98), 第5頁, 第7欄, 第3行-第6 頁, 第9欄, 第4行 (ファミリーなし)	1-11, 13-23 12
Y	J P, 10-302008, A (三菱商事株式会社), 13. 11 月. 1998 (13. 11. 98), 第9頁, 第15欄, 第33行 -第11頁, 第19欄, 第30行 (ファミリーなし)	12

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

16. 05. 00

国際調査報告の発送日

30.05.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石井 茂和



5M

8837

電話番号 03-3581-1101 内線 6438

This Page Blank (uspto)

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF RECEIPT OF
RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No.11 Mori Building
6-4, Toranomon 2-chome
Minato-ku
Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 08 March 2000 (08.03.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference SK00PCT17	International application No. PCT/JP00/00904

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

SONY CORPORATION (for all designated States except US)
KAWAKAMI, Itaru et al (for US)

International filing date : 17 February 2000 (17.02.00)
Priority date(s) claimed : 17 February 1999 (17.02.99)
Date of receipt of the record copy
by the International Bureau : 03 March 2000 (03.03.00)
List of designated Offices :

AP : GH,GM,KE,LS,MW,SD,SL,SZ,TZ,UG,ZW
EA : AM,AZ,BY,KG,KZ,MD,RU,TJ,TM
EP : AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
OA : BF,BJ,CF,CG,CI,CM,GA,GN,GW,ML,MR,NE,SN,TD,TG
National : AE,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EE,ES,FI,GB,
GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,
MW,MX,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZW

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase
☒ confirmation of precautionary designations
☐ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer: Susumu Kubo Telephone No. (41-22) 338.83.38
--	---

This Page Blank (uspto)

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

This Page Blank (uspto)

PATENT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No.11 Mori Building
6-4, Toranomon 2-chome
Minato-ku
Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 08 March 2000 (08.03.00)	
Applicant's or agent's file reference SK00PCT17	IMPORTANT NOTIFICATION
International application No. PCT/JP00/00904	International filing date (day/month/year) 17 February 2000 (17.02.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 17 February 1999 (17.02.99)
Applicant SONY CORPORATION et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
3. An asterisk(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
4. The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
17 Febr 1999 (17.02.99)	11/39218	JP	03 Marc 2000 (03.03.00)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer Susumu Kubo Telephone No. (41-22) 338.83.38
--	--

This Page Blank (uspto)

PCT COOPERATION TREATY

PCT

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No.11 Mori Building
6-4, Toranomon 2-chome
Minato-ku
Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 24 August 2000 (24.08.00)		
Applicant's or agent's file reference SK00PCT17		IMPORTANT NOTICE
International application No. PCT/JP00/00904	International filing date (day/month/year) 17 February 2000 (17.02.00)	Priority date (day/month/year) 17 February 1999 (17.02.99)
Applicant SONY CORPORATION et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

AU,KP,KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,
GE,GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,
NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
24 August 2000 (24.08.00) under No. WO 00/49510

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a **demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/00904

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/02, G06F17/60, G06F19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2000
 Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST SCIENCE & TECHNOLOGY DOCUMENT FILE, [CONTENTS*ENCIPHERMENT*ENCODING]

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-283270, A (Fujitsu Limited), 23 October, 1998 (23.10.98), page 9, Column 16, line 29 to page 14, Column 25, line 50 (Family: none)	1-11, 13-23
Y	JP, 10-269289, A (Sony Corporation), 09 October, 1998 (09.10.98), page 5, Column 7, line 3 to page 6, Column 9, line 4 (Family: none)	1-11, 13-23
Y	JP, 10-302008, A (Mitsubishi Corporation), 13 November, 1998 (13.11.98), page 9, Column 15, line 33 to page 11, Column 19, line 30 (Family: none)	12
Y		12

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not

considered to be of particular relevance

"E" earlier document but published on or after the international filing

date

"L" document which may throw doubts on priority claim(s) or which is

cited to establish the publication date of another citation or other

special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other

means

"P" document published prior to the international filing date but later

than the priority date claimed

"T" later document published after the international filing date or

priority date and not in conflict with the application but cited to

understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be

considered novel or cannot be considered to involve an inventive

step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be

considered to involve an inventive step when the document is

combined with one or more other such documents, such

combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

16 May, 2000 (16.05.00)

Date of mailing of the international search report

30.05.00

Name and mailing address of the ISA/
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.


This Page Blank (uspto)

1/5

特許協力条約に基づく国際出願願書

SK00PCT17

副本 - 印刷日時 2000年02月17日 (17.02.2000) 木曜日 14時47分57秒

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/RO/101 この特許協力条約に基づく 国際出願願書は、 右記によって作成された。	PCT-EASY Version 2.90 (updated 15.12.1999)
0-5	申立て 出願人は、この国際出願が特許 協力条約に従って処理されるこ とを請求する。	
0-6	出願人によって指定された 受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記 号	SK00PCT17
I	発明の名称	情報処理装置及び方法並びにプログラム格納媒体
II	出願人	出願人である (applicant only)
II-1	この欄に記載した者は	米国を除くすべての指定国 (all designated States except US)
II-2	右の指定国についての出願人で ある。	
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号
II-5en	Address:	7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor)
III-1-1	この欄に記載した者は	米国のみ (US only)
III-1-2	右の指定国についての出願人で ある。	
III-1-4ja	氏名 (姓名)	河上 達
III-1-4en	Name (LAST, First)	KAWAKAMI, Itaru
III-1-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号
III-1-5en	Address:	ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP

This Page Blank (uspto)

III-2 III-2-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-2-2	右の指定国についての出願人である。	米国のみ (US only)
III-2-4ja III-2-4en III-2-5ja	氏名(姓名) Name (LAST, First) あて名:	石黒 隆二 ISHIGURO, Ryuji 141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍 (国名)	日本国 JP
III-2-7	住所 (国名)	日本国 JP
III-3 III-3-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-3-2	右の指定国についての出願人である。	米国のみ (US only)
III-3-4ja III-3-4en III-3-5ja	氏名(姓名) Name (LAST, First) あて名:	田辺 充 TANABE, Mitsuru 141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-3-6	国籍 (国名)	日本国 JP
III-3-7	住所 (国名)	日本国 JP
III-4 III-4-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-4-2	右の指定国についての出願人である。	米国のみ (US only)
III-4-4ja III-4-4en III-4-5ja	氏名(姓名) Name (LAST, First) あて名:	江面 裕一 EZURA, Yuichi 141-0001 日本国 東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-4-6	国籍 (国名)	日本国 JP
III-4-7	住所 (国名)	日本国 JP

This Page Blank (uspto)

特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年02月17日 (17.02.2000) 木曜日 14時47分57秒

IV-1	代理人又は共通の代表者、 通知のあて名 下記の者は国際機関において右 記のごとく出願人のために行動 する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	小池 晃
IV-1-1en	Name (LAST, First)	KOIKE, Akira
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門二丁目6番4号 第11森ビル
IV-1-2en	Address:	No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3508-8266
IV-1-4	ファクシミリ番号	03-3508-0439
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	田村 栄一; 伊賀 誠司
IV-2-1en	Name (s)	TAMURA, Eiichi; IGA, Seiji
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国で ある他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国 である他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE 及びヨーロッパ特許条約と特許協力条約の締約国 である他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締 約国である他の国
V-2	国内特許 (他の種類の保護又は取扱いを 求める場合には括弧内に記載す る。)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-5	指定の確認の宣言 出願人は、上記の指定に加えて 、規則4.9(b)の規定に基づき、 特許協力条約のもとで認められ る他の全ての国の指定を行う。 ただし、V-6欄に示した国の指 定を除く。出願人は、これらの 追加される指定が確認を条件と していること、並びに優先日か ら15月が経過する前にその確認 がなされない指定は、この期間 の経過時に、出願人によって取 り下げられたものとみなされる ことを宣言する。	
V-6	指定の確認から除かれる国	なし (NONE)

This Page Blank (uspto)

特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年02月17日 (17.02.2000) 木曜日 14時47分57秒

VI-1	先の国内出願に基づく優先権主張		
VI-1-1	先の出願日	1999年02月17日 (17.02.1999)	
VI-1-2	先の出願番号	平成11年特許願第039218号	
VI-1-3	国名	日本国 JP	
VII-1	特定された国際調査機関 (ISA A)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	5	-
VIII-2	明細書	91	-
VIII-3	請求の範囲	8	-
VIII-4	要約	1	absk00pct17.txt
VIII-5	図面	36	-
VIII-7	合計	141	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-18	要約書とともに提示する図の番号	2	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX	提出者の記名押印		
IX-1	氏名(姓名)		
IX-2	権限		

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面:	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日 (訂正日)	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

This Page Blank (uspto)

特許協力条約に基づく国際出願願書

SK00PCT17

副本 - 印刷日時 2000年02月17日 (17.02.2000) 木曜日 14時47分57秒

国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

This Page Blank (uspto)

PATENT COOPERATION TREATY

PCT

**NOTIFICATION CONCERNING
THE FILING OF AMENDMENTS OF THE CLAIMS**
(PCT Administrative Instructions, Section 417)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira
No.11 Mori Building
6-4, Toranomom 2-chome
Minato-ku
Tokyo 105-0001
JAPON

Date of mailing (day/month/year) 04 August 2000 (04.08.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference SK00PCT17	
International application No. PCT/JP00/00904	International filing date (day/month/year) 17 February 2000 (17.02.00)
Applicant SONY CORPORATION et al	

1. The applicant is hereby notified that amendments to the claims under Article 19 were received by the International Bureau on:

31 July 2000 (31.07.00)

2. This date is within the time limit under Rule 46.1.

Consequently, the international publication of the international application will contain the amended claims according to Rule 48.2(f), (h) and (i).

3. The applicant is reminded that the international application (description, claims and drawings) may be amended during the international preliminary examination under Chapter II, according to Article 34, and in any case, before each of the designated Offices, according to Article 28 and Rule 52, or before each of the elected Offices, according to Article 41 and Rule 78.

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorised officer</p> <p>Susumu Kubo</p> <p>Telephone No.: (41-22) 338.83.38</p>
--	--

This Page Blank (uspto)

A.KOIKE & CO.

430 Rec'd PCT/PTO 28 SEP 2000

No.11 Mori Bldg., No.6-4, Toranomon 2-chome,
Minato-ku, Tokyo 105-0001 Japan

Facsimile No.81-3-3508-0439

DATE: 31 July 2000

PCT Operations Department
INTERNATIONAL BUREAU OF WIPO
34, chemin des Colombettes
1211 Geneva 20
Switzerland

Confirmation

[Amendment of the claims under Article 19(1)(Rule 46)]

Re: International Application No. PCT/JP00/00904

Applicant: Sony Corporation

Agent: KOIKE Akira, Patent Attorney
TAMURA Eiichi, Patent Attorney
IGA Seiji, Patent Attorney

International Filing Date: 17.02.00

Applicant's or Agent's File Reference: SK00PCT17

Dear Sir.

The Applicant, who has received the International Search Report relating to the above identified International Application transmitted on 30.05.00, hereby files an amendment under Article 19(1) as in the attached sheets.

Further, the applicant replaces sheet nos. 92-99 of the claims currently on file with replacement sheet nos. 92-99, 99/1, 99/2, 99/3, 99/4, 99/5, 99/6 and 99/7 supplied herewith, because the intended amendment results in adding new claims therein.

Thus claims 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 and 23 are amended, the claims 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34 and 35 are added as new claims and the original claims 1, 2 and 3 are retained unchanged.

Respectfully submitted,

A. KOIKE & CO.

田村 榮一



TAMURA Eiichi
(Patent Attorney)

Attachment: (1) Amendment under Article 19(1)

15 sheets

This Page Blank (uspto)

請求の範囲

1. コンテンツデータを蓄積する蓄積手段と、

前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、

前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含み、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御することを特徴とする情報処理装置。

2. 前記蓄積手段は、蓄積している前記コンテンツデータを管理する管理情報も蓄積しており、

前記制御手段は、前記実行手段に、前記管理情報に基づいて所定の演算を実行させることを特徴とする請求の範囲第1項に記載の情報処理装置。

3. 前記制御手段は、CPUであり、

前記蓄積手段は、ハードディスクであり、

前記実行手段は、前記制御手段としてのCPUとは別の半導体ICに組み込まれたCPUであることを特徴とする請求の範囲第1項に記載の情報処理装置。

4. (補正後) コンテンツデータ及び該コンテンツデータに付随したコンテンツ管理情報を蓄積するストレージ媒体と、

前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出

This Page Blank (uspto)

しを制御するソフトウェアからなる処理コントローラと、

前記処理コントローラから暗号化されているプログラムが供給され、該プログラムを復号して実行し、実行の結果を前記処理コントローラに供給する、前記処理コントローラとは独立した半導体チップに設けられたプログラム実行コントローラとを含み、

前記処理コントローラは、前記プログラム実行コントローラの実行結果に基づいて、前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御し、

前記プログラム実行コントローラは、その内部処理が上記半導体チップの外部からは確認不能とされ、上記コンテンツ管理情報に対する改竄確認のための演算を行うことを特徴とする情報処理装置。

5. (補正後) コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の情報処理方法において、

前記制御手段は、前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含む

ことを特徴とする情報処理方法。

6. (補正後) コンテンツデータ及び該コンテンツデータに付随したコンテンツ管理情報を蓄積するストレージ媒体と、

前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる処理コントローラと、

This Page Blank (uspto)

前記処理コントローラから暗号化されているプログラムが供給され、該プログラムを復号して実行し、実行の結果を前記処理コントローラに供給する、前記処理コントローラとは独立した半導体チップに設けられたプログラム実行コントローラとを含み情報処理装置の情報処理方法において、

前記処理コントローラは、前記プログラム実行コントローラの実行結果に基づいて、前記ストレージ媒体に対するコンテンツデータの蓄積又は読み出しを制御し、

前記プログラム実行コントローラは、その内部処理が上記半導体チップの外部からは確認不能とされ、上記コンテンツ管理情報に対する改竄確認のための演算を行うことを特徴とする情報処理方法。

7. (補正後) コンテンツデータを蓄積する蓄積手段と、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御するソフトウェアからなる制御手段と、前記制御手段から供給された、暗号化されているプログラムを復号して実行し、実行の結果を前記制御手段に供給する、前記制御手段とは独立したハードウェアに設けられた実行手段とを含む情報処理装置の前記制御手段に、

前記実行手段の実行結果に基づいて、前記蓄積手段に対する前記コンテンツデータの蓄積又は読み出しを制御する制御ステップを含むことを特徴とするコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

8. (補正後) コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

前記蓄積手段に蓄積するデータを所定の方式で圧縮する圧縮手段と、

This Page Blank (uspto)

前記蓄積手段に蓄積するデータを所定の方式で暗号化する暗号化手段と、

前記圧縮手段により圧縮され、かつ前記暗号化手段により暗号化された前記データの、前記蓄積手段に対する蓄積又は読み出しを制御する制御手段とを含むことを特徴とする情報処理装置。

9. (補正後) 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを同一の方式で圧縮又は暗号化することを特徴とする請求の範囲第8項に記載の情報処理装置。

10. (補正後) 前記圧縮手段と前記暗号化手段は、前記入力手段により入力された異なるデータを異なる方式で圧縮又は暗号化するとともに、前記蓄積手段から読み出された前記データを、予め定められている所定の装置に出力するときに、前記予め定められている共通の圧縮方式又は暗号化方式とすることを特徴とする請求の範囲第8項に記載の情報処理装置。

11. (補正後) コンテンツデータを所定の記録媒体或いはサーバから入力するインターフェースと、

前記インターフェースにより入力されたコンテンツデータを蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積するコンテンツデータを所定の方式で圧縮する圧縮プログラムと、

前記ストレージ媒体に蓄積するコンテンツデータを所定の方式で暗号化する暗号化プログラムと、

前記圧縮プログラムにより圧縮され、かつ前記暗号化プログラムにより暗号化された前記コンテンツデータの、前記ストレージ媒体に対する蓄積又は読み出しを制御するコントローラを含み、

This Page Blank (uspto)

前記圧縮プログラムと前記暗号化プログラムは、前記インターフェースにより入力された異なる方式のコンテンツデータを、同一の方式或いは異なる方式でそれぞれ圧縮又は暗号化して上記ストレージ媒体に蓄積するとともに、異なる方式で圧縮又は暗号化された前記コンテンツデータを前記ストレージ媒体から読み出して、所定のポータブルデバイスに出力するときは、所定の共通の圧縮方式又は暗号化方式となるように変換処理を行うことを特徴とする情報処理装置。

12. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含むことを特徴とする情報処理方法。

13. (補正後) コンテンツデータを所定の記録媒体或いはサーバから入力する入力ステップと、

前記入力ステップの処理で入力されたコンテンツデータをストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積したコンテンツデータを所定の方式で圧縮する圧縮ステップと、

前記圧縮ステップの処理で蓄積したコンテンツデータを所定の方

This Page Blank (uspto)

式で暗号化する暗号化ステップと、

前記圧縮ステップの処理で圧縮され、かつ前記暗号化ステップの処理で暗号化された前記コンテンツデータの、前記ストレージ媒体に対する蓄積又は読み出しを制御する制御ステップとを含み、

前記圧縮ステップと暗号化ステップは、前記入力ステップの処理で入力された異なる方式のコンテンツデータを、同一の方式或いは異なる方式でそれぞれ圧縮又は暗号化して上記ストレージ媒体に蓄積するとともに、異なる方式で圧縮又は暗号化された前記コンテンツデータを前記ストレージ媒体から読み出して、所定のポータブルデバイスに出力するときは、所定の共通の圧縮方式又は暗号化方式となるように変換処理を行うことを特徴とする情報処理方法。

14. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で圧縮する圧縮ステップと、

前記蓄積ステップの処理で蓄積されたデータを所定の方式で暗号化する暗号化ステップと、

前記圧縮ステップの処理により圧縮され、かつ前記暗号化ステップの処理により暗号化された前記データの蓄積又は読み出しを制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

15. (補正後) コンテンツデータを入力する入力手段と、

前記入力手段により入力されたデータを蓄積する蓄積手段と、

This Page Blank (uspto)

前記蓄積手段に蓄積されたデータの管理情報を保持する保持手段と、

前記保持手段に保持されている前記管理情報に基づき所定の演算を行う演算手段と、

前記演算手段の演算結果を記憶する記憶手段と、

前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結果とを比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの利用を制御する制御手段を含むことを特徴とする情報処理装置。

16. (補正後) 前記演算手段は、前記管理情報にハッシュ関数を適用して前記演算を行うことを特徴とする請求の範囲第15項に記載の情報処理装置。

17. (補正後) 前記データは音楽データであり、前記管理情報は前記音楽データを識別する識別情報を含むことを特徴とする請求の範囲第15項に記載の情報処理装置。

18. (補正後) コンテンツデータ及び該コンテンツデータにかかる識別情報を入力するインターフェースと、

前記インターフェースにより入力されたコンテンツデータを蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積されたコンテンツデータの識別情報を利用条件ファイルとして保持する第1のメモリと、

前記第1のメモリに保持されている前記識別情報にハッシュ関数を適用して演算を行う管理プログラムと、

前記管理プログラムの演算結果を記憶する第2のメモリと、

前記管理プログラムの演算結果と、前記第2のメモリに記憶され

This Page Blank (uspto)

ている過去の前記演算結果とを比較し、一致していない場合は前記ストレージ媒体に蓄積されている前記コンテンツデータのコピー或いは移動に関する処理を禁止するコントローラとを含むことを特徴とする情報処理装置。

19. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含むことを特徴とする情報処理方法。

20. (補正後) コンテンツデータ及び該コンテンツデータにかかる識別情報を入力する入力ステップと、

前記入力ステップにより入力されたコンテンツデータをストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたコンテンツデータの識別情報を利用条件ファイルとして保持する保持ステップと、

前記保持ステップの処理で保持された前記識別情報にハッシュ関数を適用して演算を行う演算ステップと、

前記演算ステップの処理での演算結果を記憶する記憶ステップと、

This Page Blank (uspto)

前記演算ステップの処理での演算結果と、前記記憶ステップの処理で記憶されている過去の前記演算結果とを比較し、一致していない場合は前記ストレージ媒体に上記蓄積ステップの処理で蓄積された前記コンテンツデータのコピー或いは移動に関する処理を禁止する制御ステップとを含むことを特徴とする情報処理方法。

21. (補正後) データを入力する入力ステップと、

前記入力ステップの処理により入力されたデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積されたデータの管理情報を保持する保持ステップと、

前記保持ステップの処理で保持された前記管理情報に基づき所定の演算を行う演算ステップと、

前記演算ステップでの演算結果を記憶する記憶ステップと、

前記演算ステップでの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

22. (補正後) 他の装置との間でデータを授受する授受手段と、

所定の固定鍵と保存用鍵を保持する保持手段と、

前記他の装置との間でデータを授受するとき、前記保持手段に保持されている前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証手段と、

前記通信用鍵を前記保存用鍵で暗号化する暗号化手段と、

This Page Blank (uspto)

前記授受手段により受信された、前記通信用鍵で暗号化されているデータを、前記暗号化手段により暗号化された前記通信用鍵と対応させて蓄積する蓄積手段とを含むことを特徴とする情報処理装置。

23. (補正後) 前記蓄積手段に蓄積されている前記通信用鍵を、前記保存用鍵を用いて復号する暗号鍵復号手段と、

前記暗号化鍵復号手段により復号された前記通信用鍵を用いて、前記蓄積手段に蓄積されているデータを復号するデータ復号手段とをさらに含むことを特徴とする請求の範囲第22項に記載の情報処理装置。

24. (追加) 接続されたポータブルデバイス或いはサーバとの間でデータを授受するインターフェースと、

所定のマスター鍵及び保存用鍵を保持するメモリと、

前記ポータブルデバイス或いはサーバとの間で上記データを授受するとき、前記メモリに保持されている前記マスター鍵を利用して、前記ポータブルデバイス或いはサーバとの間で相互認証処理を行い、通信用鍵を生成する認証プログラムと、

上記ポータブルデバイス或いはサーバから送信されたコンテンツデータを暗号化した暗号鍵を前記通信用鍵で復号し、前記保存用鍵で暗号化する暗号復号プログラムと、

前記インターフェースにより受信された、前記通信用鍵で暗号化されている上記コンテンツデータを、前記暗号復号プログラムにより復号され、上記保存用鍵で暗号化された暗号鍵と対応させて蓄積するストレージ媒体と、

前記ストレージ媒体に蓄積されている前記暗号鍵を、前記保存用鍵を用いて復号する暗号鍵復号プログラムと、

This Page Blank (uspto)

前記暗号鍵復号プログラムにより復号された前記暗号鍵を用いて、前記ストレージ媒体に蓄積されているコンテンツデータを復号するデータ復号プログラムとを含むことを特徴とする情報処理装置。

25. (追加) 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とする情報処理方法。

26. (追加) 接続されたポータブルデバイス或いはサーバとの間でデータを授受する授受ステップと、

所定のマスター鍵及び保存用鍵を保持する保持ステップと、

前記ポータブルデバイス或いはサーバとの間で上記データを授受するとき、前記保持ステップの処理で保持した前記マスター鍵を利用して、前記ポータブルデバイス或いはサーバとの間で相互認証処理を行い、通信用鍵を生成する認証ステップと、

上記ポータブルデバイス或いはサーバから送信されたコンテンツデータを暗号化した暗号鍵を前記通信用鍵で復号し、前記保存用鍵で暗号化する暗号復号ステップと、

前記授受ステップにより受信された、前記通信用鍵で暗号化され

This Page Blank (uspto)

ている上記コンテンツデータを、前記暗号復号ステップの処理により復号され、上記保存用鍵で暗号化された暗号鍵と対応させてストレージ媒体に蓄積する蓄積ステップと、

前記蓄積ステップの処理でストレージ媒体に蓄積した前記暗号鍵を、前記保存用鍵を用いて復号する暗号鍵復号ステップと、

前記暗号鍵復号ステップの処理により復号された前記暗号鍵を用いて、前記ストレージ媒体に蓄積されているコンテンツデータを復号するデータ復号ステップとを含むことを特徴とする情報処理方法。

27. (追加) 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、

前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

28. (追加) データを蓄積する蓄積手段と、

前記蓄積手段に蓄積されている前記データの利用時の条件を保持する保持手段と、

前記蓄積手段に蓄積されている前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否

This Page Blank (uspto)

かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記蓄積手段に蓄積されている前記データを前記保持手段に保持されている前記データの利用時の条件とともに前記他の装置に移転する移転手段とを含むことを特徴とする情報処理装置。

29. (追加) 前記データの利用時の条件は、再生制限条件、再生時課金条件又はコピー制限条件を含むことを特徴とする請求の範囲第28項に記載の情報処理装置。

30. (追加) コンテンツデータを蓄積するストレージデバイスと、

前記ストレージデバイスに蓄積されている前記コンテンツデータの利用条件データを保持するメモリと、

前記ストレージデバイスに蓄積されている前記コンテンツデータをポータブルデバイスに移転するとき、前記ポータブルデバイスが、前記利用条件データを充足できるか否かを判定する移転管理プログラムとを有し、

前記移転管理プログラムの判定結果において、前記ポータブルデバイスが、前記利用条件データを充足できないと判断された場合は、前記ストレージデバイスに蓄積されている前記コンテンツデータを前記ポータブルデバイスに移転することを禁止することを特徴とする情報処理装置。

31. (追加) 前記移転は、コピー、移動或いはチェックアウトを含み、前記利用条件データは、再生制限条件、再生時課金条件、又はコピー制限条件を含むことを特徴とする請求の範囲第30項に記載の情報処理装置。

This Page Blank (uspto)

3 2. (追加) データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含むことを特徴とする情報処理方法。

3 3. (追加) コンテンツデータをストレージデバイスに蓄積する蓄積ステップと、

前記ストレージデバイスに蓄積されている前記コンテンツデータの利用条件データをメモリに保持する保持ステップと、

前記ストレージデバイスに蓄積されている前記コンテンツデータをポータブルデバイスに移転するとき、前記ポータブルデバイスが、前記利用条件データを充足できるか否かを判定する判定ステップと、

前記判定ステップの判定結果において、前記ポータブルデバイスが、前記利用条件データを充足できないと判断された場合は、前記ストレージデバイスに蓄積されている前記コンテンツデータを前記ポータブルデバイスに移転することを禁止する禁止ステップとを有することを特徴とする情報処理方法。

3 4. (追加) 前記移転は、コピー、移動或いはチェックアウトを含み、前記利用条件データは、再生制限条件、再生時課金条件、又はコピー制限条件を含むことを特徴とする請求の範囲第 3 3 項に

This Page Blank (uspto)

記載の情報処理方法。

35. (追加) データを蓄積する蓄積ステップと、

前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、

前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が前記データの利用時の条件を充足できるか否かを判定する判定ステップと、

前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを前記保持ステップの処理で保持された前記データの利用時の条件とともに前記他の装置に移転する移転ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを格納したことを特徴とするプログラム格納媒体。

This Page Blank (uspio)